

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-288376

(43)Date of publication of application : 04.10.2002

(51)Int.Cl. G06F 17/60

(21)Application number : 2001-087300 (71)Applicant : SANYO ELECTRIC CO LTD

(22)Date of filing : 26.03.2001 (72)Inventor : HORI YOSHIHIRO
HIOKI TOSHIAKI

(54) CONTENTS PROVIDING METHOD AND DATA REPRODUCING DEVICE AND
DATA RECORDING DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a contents providing method for distributing enciphered contents data divided into a plurality of blocks and a plurality of licenses for decoding and reproducing the enciphered data included in those blocks.

SOLUTION: Enciphered contents data 90 or 93 obtained by enciphering music data are composed of trial enciphered music data 91 or 94 and main enciphered music data 92 or 95. The enciphered music data 91 and 94 are decoded by a license key Kc1 and the enciphered music data 92 and 95 are decoded by a license key Kc2. A distributing server holds the enciphered contents data 90 and 93 and the license keys Kc1 and Kc2 and distributes the trial enciphered music data 91 or 94 and the license key Kc1 and the main enciphered music data 92 or 95 and the license key Kc2 in this order in response to a distribution request.

CLAIMS

[Claim(s)]

[Claim 1] A contents supply method comprising:

The 1st step that receives an acquisition request of enciphered content data which enciphered contents data.

The 2nd step that provides said enciphered content data according to an acquisition request received in said 1st step.

The 3rd step that receives a providing request of the 1st license for corresponding to said some of enciphered content data and decoding said part.

The 4th step that provides said 1st license according to a providing request

received in said 3rd stepThe 5th step that receives a providing request of the 2nd license for corresponding to other parts which do not correspond to said license of the 1st of said enciphered content data unlike said 1st licenseand decoding a part besides the aboveThe 6th step that provides said 2nd license according to a providing request received in said 5th stepand the 7th step that performs accounting to offer of the 2nd license.

[Claim 2]The contents supply method according to claim 1 distributed from the server with same said enciphered content datasaid 1st licenseand said 2nd license.

[Claim 3]The contents supply method according to claim 1 with which said enciphered content data and said 1st license are distributed from the 1st serverand said 2nd license is distributed from said 1st server and the 2nd different server.

[Claim 4]The contents supply method according to claim 3 with which said enciphered content data and said 1st license are supplied to said 1st server via a recording medium.

[Claim 5]The contents supply method according to claim 1 with which said enciphered content data is provided from the 1st serverand said 1st and 2nd licenses are distributed from said 1st server and the 2nd different server.

[Claim 6]The contents supply method according to claim 5 with which said enciphered content data is supplied to said 1st server via a recording medium.

[Claim 7]In [if authentication data is received with said providing request and said authentication data is attested in said 3rd stepprovide said 1st licenseand] said 5th stepA contents supply method given in any 1 paragraph of claim 1 to claim 6 which provides said 2nd license if authentication data is received with said providing request and said authentication data is attested.

[Claim 8]It is a data reproduction apparatus which decodes enciphered content data which comprises two or more blocks according to two or more licenses corresponding to said two or more blocksand is reproducedAn interface which performs an exchange with said enciphered content data and a data recorder with which said two or more licenses were recordedHave a final controlling element for inputting directionsa contents reproduction part which decodes said enciphered content data according to said two or more licensesand is reproducedand a control sectionand said control sectionWhen encryption data contained in the n -th block (n is a natural number) that constitutes said enciphered content data in said contents reproduction part is decoded and reproduced by the n -th license corresponding to said n -th blockA data reproduction apparatus which acquires the $n+1$ st licenses from said data recorder via said interfaceand is given to said contents reproduction part.

[Claim 9]The data reproduction apparatus comprising according to claim 8:

The 1st license key attaching part holding the n -th license key with which said contents reproduction part is contained in said n -th license.

The 2nd license key attaching part holding the $n+1$ st license keys contained in said

n+1st licenses.

A decoding part which decodes encryption data which acquires selectively said n-th license key and said n+1st license keys from the said 1st and 2nd license key attaching parts and corresponds with the acquired license key.

A regenerating section which reproduces contents data decoded by said decoding part.

[Claim 10] The data reproduction apparatus according to claim 9 which said control section acquires key changed information from said data recorder via said interface chooses said n-th license key and said n+1st license keys based on said key changed information and is given to said decoding part.

[Claim 11] In a session which acquires each of a license of said plurality from said data recorder A session key generated by session key generating part which generates a different session key and said session key generating part is received Decode an encryption license key with the session key and it has further a license key decoding part which gives the decoded license key to the said 1st or 2nd license key attaching part Said control section inputs into said data recorder a session key generated by said session key generating part via said interface The data reproduction apparatus according to claim 10 which acquires an encryption license key enciphered by said session key from said data recorder via said interface and is given to said license key decoding part.

[Claim 12] From a license distributing server which provides said license key have further a data transmission and reception part which performs communication for downloading said license key and said control section When a license required in order to reproduce all of said enciphered content data is not recorded on said data recorder According to reproduction orders of said enciphered content data only a refreshable block according to said two or more licenses corresponding to said enciphered content data stored in said data recorder Acquire from said data recorder and it gives said contents reproduction part A license key corresponding to a block which constitutes said enciphered content data from said license distributing server according to acquisition directions of the new license key inputted from said final controlling element is received via said data transmission and reception part The data reproduction apparatus according to claim 8 which records the received license key on said data recorder.

[Claim 13] It is a data recorder which records two or more licenses for decoding two or more encryption data contained in enciphered content data and said two or more blocks which comprise two or more blocks A data recorder provided with a data area which stores license matching information which shows correspondence with a license area which stores said two or more licenses said enciphered content data and each of a license of said plurality and said two or more blocks which constitute said enciphered content data.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the contents supply method in the data distribution system which makes copyright protection to the copied information possible a data reproduction apparatus and a data recorder.

[0002]

[Description of the Prior Art] Each user is able to access network information easily in recent years with the terminal for the individuals [progress / of digital information communications networkssuch as the Internetetc.] using a portable telephone etc.

[0003] In such a digital information communications network information is transmitted by a digital signal. Therefore it is possible to perform a copy of data without producing most degradation of the tone quality by such a copy or image quality even when an individual user copies the music and picture image data which were transmitted for example in the above information-and-telecommunications networks.

[0004] Therefore if the policy for suitable copyright protection is not taken when the contents data in which the right of authorssuch as music data and image data exists on such a digital information communications network is transmitted there is a possibility of infringing on right of an owner of a copyright remarkably.

[0005] On the other hand supposing it cannot give top priority to the purpose of copyright protection and cannot distribute contents data via the digital information communications network to expand rapidly it will become rather disadvantageous also for the owner of a copyright who can collect a fixed royalty when reproducing contents data fundamentally.

[0006] If it thinks and sees here not taking the case of distribution through the above digital information communications networks but taking the case of the recording medium which recorded digital data Usually about CD (compact disk) which recorded the music data currently sold the copy of the music data from CD to magneto-optical discs (MD etc.) can be freely performed in principle as long as the copied music concerned is stopped to individual use. However the individual user who performs digital sound recording etc. is to pay an owner of a copyright indirectly the constant sum of the prices for mediasuch as digital-sound-recording apparatus itself and MD as guarantee money.

[0007] And when the music data which is a digital signal is copied to MD from CD it has come to be unable to perform copying music information to MD of further others as digital data from recordable MD on the composition of apparatus in view of these information being the digital data which does not almost have copy degradation for copyright protection.

[0008] Since distributing music data and image data to the public through a digital

information communications network also from such a situation is an act from which itself receives restriction by rights of public transmission of an owner of a copyrightsufficient policy for copyright protection needs to be devised.

[0009]In this caseit is necessary for the contents data received once to prevent being reproduced still more freely about the contents data of music dataimage dataetc. which is works transmitted to the public through a digital information communications network.

[0010]Then the data distribution system with which the distributing server holding the enciphered content data which enciphered contents data distributes enciphered content data via a terminal unit to the memory card with which terminal unitssuch as a portable telephonerewere equipped is proposed. In this data distribution systemthe open encryption key and certificate of the memory card beforehand attested by the certificate authority are transmitted to a distributing server in the case of the distribution request of enciphered content dataAfter checking having received the certificate in which the distributing server was attestedthe license key for decoding enciphered content data and enciphered content data to a memory card is transmitted. And when distributing enciphered content data and a license keya distributing server and a memory card generate a different session key for every distributionwith the generated session keyencipher an open encryption key and exchange keys a distributing server and between memory cards.

[0011]Eventually a distributing server transmits the license which it was enciphered with the open encryption key of memory card eachand was further enciphered with the session keyand enciphered content data to a memory card. And a memory card records the license and enciphered content data which were received.

[0012]And a portable telephone is equipped with a memory card when reproducing the enciphered content data recorded on the memory card. A portable telephone also has a dedicated communication circuit for decoding the enciphered content data from a memory card other than the usual telephone functionand reproducingand outputting to the exterior.

[0013]Thusthe user of a portable telephone can receive enciphered content data from a distributing server using a portable telephoneand can reproduce the enciphered content data.

[0014]In distribution of enciphered content datamusic data is divided into the encrypted music data for an auditionand the encrypted music data for distributionfor exampleFirstdistributing the music data for an auditionand distributing the encrypted music data for distribution and a licensewhen you wish the encrypted music data for distribution and distribution of a license as a result of decoding and reproducing and a user's trying listening the music data for an audition is performed. In such a casethe music data for an audition is inferior in tone quality compared with the music data for main partsand even if it downloads the music data for an auditionit spoils right of an owner of a copyright.

[0015]

[Problem(s) to be Solved by the Invention]However although specification of the music data which it is going to purchase with the music data for an audition for a user is possible it cannot check about the tone quality of the music data for distribution provided. There is no guarantee with same music data for an audition and music data for distribution.

[0016]Such a problem is similarly produced in distribution of the contents data of not only music data but reading data teaching-materials data a video data a game etc.

[0017]In the contents data of reading data teaching-materials data a game etc. Not all data is purchased by package but when responding for every stage for every chapter in reading data accepting a user's distribution request in teaching-materials data or a game and distributing it originates in the distribution performed by dividing into multiple times and the problem that the batch management of contents data becomes difficult occurs for example.

[0018]then this invention is made in order to solve this problem and it comes out. The purpose is to provide the contents supply method which distributes two or more licenses for decoding and reproducing the enciphered content data divided into the field of ** and the encryption data contained to two or more fields.

[0019]Another purpose of this invention is to provide a refreshable data reproduction apparatus for the enciphered content data divided into two or more fields according to two or more licenses.

[0020]Another purpose of this invention is to provide the data recorder which recorded the enciphered content data divided into two or more fields and two or more licenses.

[0021]

[Means for Solving the Problem]According to this invention a contents supply method is provided with the following.

The 1st step that receives an acquisition request of enciphered content data which enciphered contents data.

The 2nd step that provides enciphered content data according to an acquisition request received in the 1st step.

The 3rd step that receives a providing request of the 1st license for corresponding to some enciphered content data and decoding a part.

The 4th step that provides the 1st license according to a providing request received in the 3rd step The 5th step that receives a providing request of the 2nd license for corresponding to other parts which do not correspond to a license of the 1st of enciphered content data unlike the 1st license and decoding other parts The 6th step that provides the 2nd license according to a providing request received in the 5th step and the 7th step that performs accounting to offer of the 2nd license.

[0022]Preferably enciphered content data the 1st license and the 2nd license are distributed from the same server.

[0023] Preferably enciphered content data and the 1st license are distributed from the 1st server and the 2nd license is distributed from the 1st server and the 2nd different server.

[0024] Preferably enciphered content data and the 1st license are supplied to the 1st server via a recording medium.

[0025] Preferably enciphered content data is provided from the 1st server and the 1st and 2nd licenses are distributed from the 1st server and the 2nd different server.

[0026] Preferably enciphered content data is supplied to the 1st server via a recording medium.

[0027] Preferably in the 3rd step if authentication data is received with a providing request and authentication data is attested the 1st license is provided and in the 5th step if authentication data is received with a providing request and authentication data is attested the 2nd license is provided.

[0028] According to this invention a data reproduction apparatus. It is a data reproduction apparatus which decodes enciphered content data which comprises two or more blocks according to two or more licenses corresponding to two or more blocks and is reproduced. An interface which performs an exchange with enciphered content data and a data recorder with which two or more licenses were recorded. Have a final controlling element for inputting directions a contents reproduction part which decodes enciphered content data according to two or more licenses and is reproduced and a control section and a control section. When encryption data contained in the n -th block (n is a natural number) that constitutes enciphered content data in a contents reproduction part is decoded and reproduced by the n -th license corresponding to the n -th block. The $n+1$ st licenses are acquired from a data recorder via an interface and it gives a contents reproduction part.

[0029] The 1st license key attaching part that holds preferably the n -th license key with which a contents reproduction part is contained in the n -th license. The 2nd license key attaching part holding the $n+1$ st license keys contained in the $n+1$ st licenses. The n -th license key and the $n+1$ st license keys are selectively acquired from the 1st and 2nd license key attaching parts and a decoding part which decodes encryption data corresponding with the acquired license key and a regenerating section which reproduces contents data decoded by decoding part are included.

[0030] Preferably a control section acquires key changed information from a data recorder via an interface chooses the n -th license key and the $n+1$ st license keys based on key changed information and gives them to a decoding part.

[0031] In a session which acquires each of two or more licenses from a data recorder preferably a session key generated by session key generating part which generates a different session key and a session key generating part is received. Decode an encryption license key with the session key and it has further a license key decoding part which gives the decoded license key to the 1st or 2nd license key attaching part. A control section inputs into a data recorder a session key generated by a session key generating part via an interface acquires an encryption license key

enciphered by a session key from a data recorder via an interface and gives it to a license key decoding part.

[0032] Preferably from a license distributing server which provides a license key a data reproduction apparatus is further provided with a data transmission and reception part which performs communication for downloading a license key and a control section. When a license required in order to reproduce all of enciphered content data is not recorded on a data recorder, according to reproduction orders of enciphered content data, only a refreshable block according to two or more licenses corresponding to enciphered content data stored in a data recorder. Acquire from a data recorder, give a contents reproduction part and a license key corresponding to a block which constitutes enciphered content data from a license distributing server according to acquisition directions of the new license key inputted from a final controlling element is received via a data transmission and reception part. The received license key is recorded on a data recorder.

[0033] According to this invention, a data recorder. It is a data recorder which records two or more licenses for decoding two or more encryption data contained in enciphered content data and two or more blocks which comprise two or more blocks. It has a data area which stores license matching information which shows correspondence with a license area which stores two or more licenses, enciphered content data, and each of two or more licenses and two or more blocks which constitute enciphered content data.

[0034]

[Embodiment of the Invention] It explains in detail, referring to drawings for an embodiment of the invention. Identical codes are given to a portion same in the inside of a figure or considerable and the explanation is not repeated.

[0035] Drawing 1 is a schematic diagram for explaining notionally the entire configuration of the data distribution system with which the data recorder by this invention acquires enciphered content data.

[0036] To the memory card 110 equipped with digital music data by the user's portable telephone via the portable telephone network below. Or although explained taking the case of the composition of the data distribution system distributed to the memory card 110 equipped with digital music data by the card writer via the Internet. When distributing the contents data as other works, for example, image data, dynamic image data, etc., this invention can be applied without being limited in such a case so that it may become clear by the following explanation.

[0037] With reference to drawing 1, the distribution career 20 relays the distribution request (distribution request) from a user obtained through the self portable telephone network to the distributing server 10. The distributing server 10 which manages the music data in which copyright exists. [whether the memory card 110 with which the portable telephone user's portable telephone 100 accessed in quest of data distribution was equipped has just authentication data and]
Namely, authenticating processing of whether to be the regular memory card provided

with the contents protection feature is performed. Such enciphered content data and a license are given to the cellular phone company which is the distribution career 20 which distributes the license for decoding enciphered content data to a regular memory card.

[0038] The distribution career 20 distributes enciphered content data and a license via a portable telephone network and the portable telephone 100 to the memory card 110 with which the portable telephone 100 which transmitted the distribution request through the self portable telephone network was equipped.

[0039] In drawing 1 it has the composition that a portable telephone user's portable telephone 100 is equipped with the removable memory card 110 for example. The memory card 110 receives the enciphered content data received by the portable telephone 100 and after it decodes the encryption performed in the above-mentioned distribution it gives it to the music reproduction section (not shown) in the portable telephone 100.

[0040] Furthermore -- a portable telephone user passes the head telephone 130 grade linked to the portable telephone 100 for example -- such contents data -- " -- reproducing carrying out and hearing is possible.

[0041] By having such composition, first, if the memory card 110 is not used, in response to distribution of contents data, it will become difficult composition from the distributing server 10 to play music.

[0042] By and the thing for which the frequency is calculated in the distribution career 20 whenever it distributes the contents data for one music. If the distribution career 20 presupposes that the royalty generated whenever a portable telephone user receives contents data (download) is collected with the phonecall charges of a portable telephone, it will become easy for an owner of a copyright to secure a royalty.

[0043] In the data distribution system shown in drawing 1 enciphered content data {Dc} Kc Audition field {Dc1} Kc1 to which encryption which can be decoded in license key Kc1 was given and which is a field and body area {Dc2} Kc2 as which it was enciphered in license key Kc2 are comprised and it is constituted as one enciphered content data. Therefore the license for an audition containing license key Kc1 is required for an audition and the license for an audition and the license for main parts containing license key Kc2 are required for reproduction of the whole contents.

[0044] The distributing server 10 distributes first the license for an audition containing enciphered content data {Dc} Kc and license key Kc1 to the portable telephone 100 via a portable telephone network. And in the contents playback circuit (not shown) where the portable telephone 100 was equipped with the user Enciphered content data {Dc} If it wants for audition field {Dc1} Kc1 which is a part of Kc to be decoded by license key Kc1 of the license for an audition to listen to the played music and to download these contents Again the distribution request of the license for main parts is transmitted to the distributing server 10. And the distributing server 10 distributes the license for main parts which contains license

key Kc2 according to the received distribution request to the portable telephone 100 via a portable telephone network.

[0045] If it does so the contents playback circuit of the portable telephone 100 can reproduce all the enciphered content data {Dc} Kc(s) using license key Kc1 contained in the license for an audition and license key Kc2 which are contained in the license for main parts.

[0046] In drawing 1 the distributing server 10 distributes the license for an audition containing enciphered content data {Dc} Kc and license key Kc1 to the personal computer 50 via Internet network 30. And the personal computer 50 receives the distribution request of the license for an audition which contains encrypted-music-data {Dc} Kc and license key Kc1 via the USB (Universal Serial Bus) cable 70 and the card writer 80. It judges by the same method as having mentioned above the justification of the memory card 110 with which the card writer 80 was equipped and the license for an audition which contains encrypted-music-data {Dc} Kc and license key Kc1 in a regular memory card is recorded. And the memory card 110 is extracted from the card writer 80 and the portable telephone 100 is equipped with it. The user of the portable telephone 100 reads encrypted-music-data {Dc} Kc and license key Kc1 from the memory card 110 with which it was equipped and it decodes and reproduces and he tries listening field {Dc1} Kc1 which can be decoded by license key Kc1 which is a part of encrypted-music-data {Dc} Kc. And a user transmits the distribution request of the license for main parts which contains license key Kc2 to the distributing server 10 via the portable telephone network 30 when you wish download of the license for main parts containing license key Kc2 in order to reproduce all the encrypted-music-data {Dc} Kc(s). If it does so the distributing server 10 will distribute the license for main parts containing license key Kc2 to the portable telephone 100 via a portable telephone network after checking again that it is a memory card with the regular memory card 110. And the portable telephone 100 records the license for main parts containing license key Kc2 which received on the memory card 110. The whole encrypted-music-data {Dc} Kc by which the user was recorded on the memory card 110 using the portable telephone 100 is decoded and reproduced using license key Kc1 and license key Kc2.

[0047] The license for an audition containing license key Kc1 for CD-ROM 60 to decode audition field {Dc1} Kc1 of enciphered content data {Dc} Kc and enciphered content data {Dc} Kc is recorded. The personal computer 50 reads enciphered content data {Dc} Kc and the license for an audition from CD-ROM 60. And the personal computer 50 checks the justification of the memory card 110 with which the card writer 80 was equipped via the card writer 80 and USB cable 70 and records the license for an audition which contains license key Kc1 in a regular memory card. And the memory card 110 is extracted from the card writer 80 and the portable telephone 100 is equipped with it. The user of the portable telephone 100 reads audition field {Dc1} Kc1 and license key Kc1 which are a part of encrypted-music-data {Dc} Kc from the memory card 110 with which it was equipped is decoded and

reincarnated and tries listening a part of encrypted-music-data {Dc} Kc. And a user transmits the distribution request of the license for main parts which contains license key Kc2 to the distributing server 10 via the portable telephone network 30 when you wish download of the license for main parts containing license key Kc2. [0048] If it does so the distributing server 10 will distribute the license for main parts containing license key Kc2 to the portable telephone 100 via a portable telephone network after checking that the memory card 110 is a regular memory card. And the portable telephone 100 records license key Kc2 which received on the memory card 110. A user reads encrypted-music-data {Dc} Kc [which was recorded on the memory card 110 using the portable telephone 100] and license key Kc1 and license key Kc2 and reproduces all the enciphered content data {Dc} Kc(s).

[0049] At this time the license for an audition currently recorded on CD-ROM 60 can be accessed now only by the exclusive program for being recorded after being enciphered and recording a license on the memory card 110. Even if it reproduces the license on CD-ROM 60 as it is it cannot use for reproduction of enciphered content data {Dc} Kc.

[0050] Only encrypted-music-data {Dc} Kc is recorded CD-ROM 60. The personal computer 50 reads encrypted-music-data {Dc} Kc from CD-ROM 60. And the personal computer 50 records encrypted-music-data {Dc} Kc on the memory card 110 via the card writer 80 and USB cable 70. And the memory card 110 is extracted from the card writer 80 and the portable telephone 100 is equipped with it. The user of the portable telephone 100 demands the distribution of the license for an audition to encrypted-music-data {Dc} Kc recorded on the memory card 110 with which it was equipped of the distributing server 10 via a portable telephone network and the distribution career 20.

[0051] In the data distribution system shown in drawing 1 enciphered content data {Dc} Kc Audition field {Dc1} Kc1 to which encryption which can be decoded in license key Kc1 was given and which is a field and body area {Dc2} Kc2 as which it was enciphered in license key Kc2 are comprised and it is constituted as one enciphered content data. Therefore the license for an audition containing license key Kc1 is required for an audition and the license for an audition and the license for main parts containing license key Kc2 are needed for reproduction of the whole contents.

[0052] The distributing server 10 distributes first the license for an audition containing enciphered content data {Dc} Kc and license key Kc1 to the portable telephone 100 via a portable telephone network. And in the contents playback circuit (not shown) where the portable telephone 100 was equipped with the user Enciphered content data {Dc} If field {Dc1} Kc1 for an audition which is a part of Kc wants to listen to the music which was decoded by license key Kc1 of the license for an audition and was played and to download these contents Again the distribution request of the license for main parts is transmitted to the distributing server 10. And the distributing server 10 distributes the license for main parts which contains license key Kc2 according to the received distribution request to the

portable telephone 100 via a portable telephone network.

[0053] If it does so the contents playback circuit of the portable telephone 100 can reproduce all the enciphered content data {Dc} Kc(s) using license key Kc1 contained in the license for an audition and Kc2 which are contained in the license for main parts.

[0054] Although explanation is omitted the personal computer 50 can acquire the license for main parts as well as the license for an audition via Internet network 30 and it can also be made to record on the memory card 110. Encryption communication is used when distributing the license for an audition or the license for main parts to the personal computer 50 via Internet network 30.

[0055] Thus the memory card 110 acquires the license for main parts containing the license for an audition and license key Kc2 which contain encrypted-music-data {Dc} Kc and license key Kc1 by various kinds of methods.

[0056] Being needed on a system in order to make refreshable the contents data enciphered and distributed in composition as shown in drawing 1 at the user side of a portable telephone are a method for distributing the license key in communication to the 1st and to the further 2nd. It is the method itself which enciphers contents data to distribute and is the composition of realizing contents data protection for preventing further the unapproved copy of the contents data distributed to the 3rd in this way.

[0057] In the time of distribution and generating of each reproductive session especially in an embodiment of the invention the recorder and data reproduction terminal (the data reproduction terminal which can reproduce contents is also called portable telephone.) in which the attestation and the check function to the movement destination of these contents data were enriched and un-attesting or a decode key was torn the following -- it is the same -- by preventing the output of the contents data to receive explains the composition which strengthens the copyright protection of contents data.

[0058] In the following explanation from the distributing server 10 via each portable telephone to a memory card. Or suppose that the processing which transmits contents data (enciphered content data and license) to a memory card via a card writer from a personal computer is called "distribution."

[0059] In the data distribution system shown in drawing 1 drawing 2 is a figure explaining the characteristics such as data for the communication used and information.

[0060] First the data distributed from the distributing server 10 is explained. Dc(s) are contents data of music data etc. Encryption which can decode the contents data Dc with the license key Kc is given. The contents data Dc comprises audition field Dc1 and body area Dc2 and is enciphered by a different encryption key respectively. The encryption which can be decoded by license key Kc1 audition field Dc1 as audition field {Dc1} Kc1 given body area Dc2 One enciphered content data {Dc} Kc is constituted as body area {Dc2} Kc2 to which encryption which can be decoded by

license key Kc2 was given. The contents data Dc is certainly distributed to the portable telephone 100 or the personal computer 50 as enciphered content data {Dc} Kc. As a result, the whole contents data Dc is supplied widely from the distributing server 10 as enciphered content data {Dc} Kc to which encryption which can be decoded with the license key Kc (Kc1 and Kc2 are comprised) was given. [0061] In the following, it shall be shown that the notation {Y} X gave encryption which can be decoded with the decode key X for the data Y.

[0062] With reference to drawing 3, the format of enciphered content data {Dc} Kc which the information database 304 holds is explained. Enciphered content data {Dc} Kc When Kc is encrypted music data, enciphered content data {Dc} Kc comprises the format shown in (a) of drawing 3. The encrypted music data 90 comprises the audition field 91 ({Dc1} Kc1) and the body area 92 ({Dc2} Kc2). The audition field 91 ({Dc1} Kc1) can be decoded by license key Kc1. The body area 92 ({Dc2} Kc2) can be decoded by license key Kc2. The audition field 91 ({Dc1} Kc1) is included in the middle of enciphered content data {Dc} Kc and the body area 92 ({Dc2} Kc2) is divided into two. In this case, the encrypted music data 91 for an audition comprises the rest of music. Although the audition field 91 ({Dc1} Kc1) was shown as one continuous field, they may be the body area 92 ({Dc2} Kc2) and a field similarly divided by the body area 92 ({Dc2} Kc2).

[0063] Enciphered content data {Dc} Kc may comprise the format shown in (b) of drawing 3. The encrypted music data 93 comprises the encrypted music data 94 for an audition and the encrypted music data 95 for main parts. The encrypted music data 94 for an audition can be decoded by license key Kc1. The encrypted music data 95 for main parts can be decoded by license key Kc2. The encrypted music data 94 for an audition is contained in the beginning of enciphered content data {Dc} Kc. In this case, the encrypted music data 94 for an audition comprises the intro of music.

[0064] With reference to drawing 4, generation of enciphered content data {Dc} Kc84 is explained. It divides into block BLK1 which has the fixed length of the M byte which is the minimum encryption unit about source data Dc81 which is contents data of a plaintext BLK2...BLKk and the block data 82 is generated (k is a natural number). When final block BLKk is less than a M byte, dummy data without a meaning is added to a data end and the block of a M byte is constituted (slash part). And each of block BLK1 BLK2...BLKk is enciphered separately and the encryption data 83 is generated. At this time, it is determined whether it is made to correspond to any of license key Kc1 and Kc2 for every block. Correspondence with a license key and a block is recorded as license key matching information in additional information Dc-inf. Then a header is added to each of block BLK1 BLK2...BLKk and enciphered content data {Dc} Kc84 is generated. That is, block BLK1 comprises the header 841 and the encryption data 842, block BLK2 comprises the header 843 and the encryption data 844 and the block BLKk comprises the header 845 and the

encryption data 846. The header 841843845 is N byte's data and the scramble flag which shows whether the block is an encryption block or it is a non-enciphering block is recorded. That is the header 841843845 contains "0" which shows that it is "1" or the non-enciphering block which shows that it is an encryption block. Therefore the enciphered content data which drawing 3 shows comprises the data format shown in drawing 4 and an audition field and a body area are constituted by two or more blocks not overlapping.

[0065] Again with reference to drawing 2 additional information Dc-inf as plaintext information including the license key matching information over enciphered content data the information about the copyright of contents data or server access pertinent information is distributed with enciphered content data from the distributing server 10. License ID which is the management codes for specifying license key Kc the license key from the distributing server 10 etc. as a license The distributing server 10 It is exchanged between the portable telephone 100 or the personal computer 50 and is recorded on the memory card 110 with the license key Kci. The content ID which is a code for identifying the contents data Dc as a license. Are generated based on the license terms of purchase AC included the information including the kind of license functional limitation etc. determined by the specification from the user side. The reproduction control information ACp etc. which are the access control information ACm which is information about the restriction to access of the license in a recorder (memory card) and the control information about the reproduction in a data reproduction terminal exist. The access control information ACm is control information which is in charge of outputting the license or license key from a memory card outside and specifically there are the number of times (number which outputs a license key for reproduction) of refreshable limitation information about movement and the duplicate of a license etc. In order to reproduce the reproduction control information ACp after a contents playback circuit receives a license key it is the information which restricts reproduction and a reproduction term reproduction speed change restrictions reproduction range specification (partial license) etc. occur.

[0066] Henceforth suppose that content ID the license key Kci ($i = 12$) license ID the access control information ACm and the reproduction control information ACp are combined and it is named a license generically. The license containing license key Kc1 is a license for an audition and the license containing license key Kc2 is a license for main parts.

[0067] the reproduction frequency (0: reproduction improper.) which is the control information to which the access control information ACm restricts reproduction frequency henceforth for simplification having the number of times of 1 - 254: refreshable and no 255: restrictions and movement / duplicate flag (1: move duplicate improper.) which restricts movement and the duplicate of a license 2: Using only movement as the dyadic eye of good and 3: move duplication prohibition the reproduction control information ACp shall restrict only the reproduction term (UTC time code) which is the control information which specifies a

refreshable term.

[0068] Drawing 5 is a figure explaining the characteristics such as data for the attestation used in the data distribution system shown in drawing 1 and information.

[0069] The open encryption keys KPpy and KPMw peculiar to a contents playback circuit and a memory card are formed respectively. The open encryption keys KPpy and KPMw can be decoded respectively with the secret decode key Kpy peculiar to a contents playback circuit and the secret decode key Km w peculiar to a memory card. These public presentation encryption key and a secret decode key have a contents playback circuit and a different value for every kind of memory card. These open encryption keys and secret decode keys are named generically a class key is called and the unit which shares a class public presentation encryption key for these open encryption keys and shares a class secret decode key and a class key for a secret decode key is called a class. A class changes with the kind of a manufacturing company or product lots at the time of manufacture etc.

[0070] Cpy is provided as a class certificate of a contents playback circuit (a portable telephone or a reproduction terminal) and Cmw is provided as a class certificate of a memory card. These class certificates have a contents playback circuit and different information for every class of a memory card. The Tampa-proof module is torn or the code with a class key was broken namely to the class which the secret decode key revealed it is listed by prohibition class lists and is the prohibition target of license acquisition.

[0071] The class public presentation encryption key and class certificate of these contents playback circuits Authentication data {KPpy//Cpy} In the form of KPpy the class public presentation encryption key and class certificate of a memory card are recorded [in the form of authentication data {KPMw//Cmw} KPa] on a data reproduction circuit and a memory card respectively at the time of shipment. Although it will explain to details later KPa is an open authentication key common to the whole distribution system.

[0072] The secret decode key Kmcx peculiar to each which can decode the data enciphered as a key for managing data processing in the memory card 110 with the open encryption key KPMcx set up for every medium and the open encryption key KPMcx which are called a memory card exists. An individual open encryption key and secret decode key are named generically for every memory card of this an individual key is called the open encryption key KPMcx is called an individual public presentation encryption key and the secret decode key Kmcx is called an individual secret decode key.

[0073] As an encryption key for the maintenance of secret in the data transfer in the data transfer between the outside of a memory card and a memory card Whenever distribution of contents data and reproduction are performed the distributing server 10 the portable telephone 100 and the common keys Ks1-Ks3 generated in the memory card 110 are used.

[0074] Here the common keys Ks1-Ks3 are a unit of communication between a

distributing server a contents playback circuit or a memory card or a unit of access --
"-- it being a peculiar common key by which it is generated in every
session" and Suppose that these common keys Ks1-Ks3 are also called a "session
key" to below.

[0075] These session keys Ks1-Ks3 are managed with a distributing server a contents
playback circuit and a memory card by having a peculiar value for every session.
Specifically session key Ks1 is generated for every distribution session by a
distributing server. Session key Ks2 is generated for every distribution session and
reproduction session with a memory card and session key Ks3 is generated for every
reproduction session in a contents playback circuit. In each session the security
intensity in a session can be raised by delivering and receiving these session
keys and transmitting a license key etc. in response to the session key generated by
other apparatus after performing encryption by this session key.

[0076] In communication between the personal computer 50 and the memory card
110 via the card writer 80 and USB cable 70 Reading ***** is [function / of the
distributing server 10 and the portable telephone 100] good for the card writer 80
and USB cable 70 in the personal computer 50 in ***** and the memory card
interface 1200.

[0077] Drawing 6 is a schematic block diagram showing the composition of the
distributing server 10 shown in drawing 1. The distributing server 10 is provided with
the following.

The information database 304 for holding delivery information which enciphered
contents data according to the prescribed methods such as data and content ID.
The charge database 302 for holding the accounting information which followed the
access start to contents data for every user of a portable telephone.
The menu database 307 holding the menu of the contents data held at the
information database 304.

The distribution recording data base 308 holding the log about distribution of
transaction ID etc. which specify distribution of contents data a license key etc. for
every distribution of a license The data processing part 310 for receiving the data
from the information database 304 the charge database 302 the menu database
307 and the distribution recording data base 308 via bus BS1 and performing
predetermined processing The communication apparatus 350 for performing data
transfer between the distribution career 20 and the data processing part 310 via a
communications network.

[0078] Enciphered content data {Dc} When Kc is reading data teaching-materials
data or data of game software enciphered content data {Dc} Kc comprises the format
shown in (c) of drawing 13. The enciphered content data 96 comprises two or more
fields 961-967. Each fields 961-967 can be decoded by license key
Kc1 Kc2 Kc3 Kc4 Kc5 Kc6 and Kc7 respectively.

[0079] Enciphered content data {Dc} When it is the video data on which Kc tried like

the already explained music data and which it equipped with the field [like] enciphered content data [Dc] Kc comprises the format shown in (d) of drawing 13. The encryption data 97 comprises the field 971 for attachment and the field 972 for main parts. The field 971 for attachment can be decoded by license key Kc1. The field 972 for main parts can be decoded by license key Kc2. The field 971 for attachment comprises the subtitle of video or a game. About decoding of the enciphered content data 96 and 97 the contents playback circuit 1550 shown in drawing 7 is acceptable. In this case the music reproduction section 1520 is transposed to the regenerative circuit which suited each contents.

[0080] The data processing part 310 is provided with the following.

The distribution control part 315 for controlling operation of the data processing part 310 according to the data on bus BS1.

The session key generating part 316 for being controlled by the distribution control part 315 and generating session key Ks1 at the time of a distribution session.

The authentication key attaching part 313 holding two kinds of open authentication keys KPa for decoding authentication data {KPMw//Cmw} KPa for the attestation sent from the memory card.

Authentication data {KPMw//Cmw} KPa for the attestation sent from the memory card is received via communication apparatus 350 and bus BS1. The decoding processing section 312 which performs decoding processing with the open authentication key KPa from the authentication key attaching part 313. Session key Ks1 generated from the session key generating part 316 which generates session key Ks1 and the session key generating part 316 is enciphered using the class public presentation encryption key KPMw obtained by the decoding processing section 312 for every distribution session. The enciphering processing part 318 for outputting to bus BS1 and the decoding processing section 320 which performs decoding processing in response to the data transmitted after being enciphered by session key Ks1 from bus BS1.

[0081] The data processing part 310 is provided with the following.

The enciphering processing part 326 for enciphering the license key Kc and the access control information ACm which are given from the distribution control part 315 with the individual public presentation encryption key KPMcx for every memory card obtained by the decoding processing section 320.

The enciphering processing part 328 for enciphering further and outputting the output of the enciphering processing part 326 to bus BS1 by session key Ks2 to which it is given from the decoding processing section 320.

[0082] The operation in the distribution session of the distributing server 10 will be later explained in detail using a flow chart.

[0083] Drawing 7 is a schematic block diagram for explaining the composition of the portable telephone 100 shown in drawing 1.

[0084]The portable telephone 100 is provided with the following.
Bus BS2 for performing data transfer of each part of the portable telephone 100.
The antenna 1101 for receiving the signal by which wireless transfer is carried out with a portable telephone network.
The transmission and reception section 1102 for changing into a baseband signal in response to the signal from an antenna or modulating the data from a portable telephone and giving the antenna 1101.

[0085]The portable telephone 100 is provided with the following.
The microphone 1103 for incorporating the voice data of the user of the portable telephone 100.
A/D converter 1104 which changes the voice data from the microphone 1103 into a digital signal from an analog signal.
The audio coding section 1105 which modulates the voice data from A/D converter 1104 to a prescribed method.

[0086]The cellular-phone machine 100 is provided with the following.
The sound reproduction section 1106 which reproduces the voice data of the user of other portable telephones who received via the antenna 1101 and the transmission and reception section 1102.
DA converter 1107 which changes the data from the sound reproduction section 1106 into an analog signal from a digital signal.
The loudspeaker 1108 which outputs the voice data from DA converter 1107 to the exterior.

[0087]The portable telephone 100 is provided with the following.
The controller 1109 for controlling operation of the portable telephone 100 via bus BS2.
The navigational panel 1111 for giving the directions from the outside to the portable telephone 100.
The display panel 1110 for giving a user the information outputted from controller 1109 grade as vision information.

[0088]The portable telephone 100 is provided with the following.
The removable memory card 110 for memorizing the contents data (music data) from the distributing server 10 and performing decoding processing.
The memory card interface 1200 for controlling transfer of the data between the memory card 110 and bus BS2.

[0089]The portable telephone 100 contains the authentication data attaching part 1500 holding authentication data [KPp1//Cp1] KPp1 enciphered in the state where the justification can be further attested by decoding class public presentation

encryption key K_{Pp1} and class certificate C_{p1} with the open authentication key K_{Pa}. Here the class y of the reproduction terminal 102 presupposes that it is y = 1.

[0090] The portable telephone 100 is provided with the following.

The K_{p1} attaching part 1502 holding K_{p1} which is a decode key peculiar to a class. The decoding processing section 1504 which obtains session key K_{s2} which decoded the data which received from bus BS2 by K_{p1} and was generated by the memory card 110.

[0091] The portable telephone 100 further The session key generating part 1508 which generates session key K_{s3} for enciphering the data which sets and is carried out on bus BS2 between the memory cards 110 in the reproduction session which reproduces the contents data memorized by the memory card 110 with a random number etc. In the reproduction session of enciphered content data it is the license key K_c (K_{c1} and K_{c2} are comprised.) from the memory card 110. It is below the same and when receiving the reproduction control information A_{Cp} session key K_{s3} generated by the session key generating part 1508 is enciphered by session key K_{s2} obtained by the decoding processing section 1504 and the enciphering processing part 1506 outputted to bus BS2 is included.

[0092] The portable telephone 100 is provided with the following.

The decoding processing section 1510 which decodes the data on bus BS2 by session key K_{s3} and outputs the license key K_c and the reproduction control information A_{Cp}.

K_c either one of license key K_{c1} outputted from the decoding processing section 1510 or 2 is outputted to the K_c attaching part 1514 via the terminal 1512 with the directions from the controller 1109. The terminal 1513 is passed and license key K_{c1} and K_{c2} are the switches 1511 which output another side to the K_c attaching part 1515 either.

[0093] The portable telephone 100 is provided with the following.

The K_c attaching part 1514 holding K_c either license key K_{c1} inputted from the terminal 1512 or 2.

The K_c attaching part 1515 which holds license key K_{c2} when the different license key 1514 from the license key which the K_c attaching part 1514 inputted from the terminal 1513 holds i.e. K_c attaching part holds license key K_{c1}.

[0094] The portable telephone 100 includes the switch 1518 which chooses further any one of two license key K_{c1} held at the K_c attaching part 1514 or the K_c attaching part 1515 and the K_{c2} and is outputted to the decoding processing section 1519. The switch 1518 is provided with the following.

The terminal 1516 which receives the license key from the K_c attaching part 1514. The terminal 1517 which receives the license key from the K_c attaching part 1515. With the directions from the controller 1109 the switch 1518 chooses the terminal

1516 or the terminal 1517 and outputs license key Kc1 or license key Kc2 to the decoding processing section 1519.

[0095] The portable telephone 100 contains the decoding processing section 1519 which decodes enciphered content data {Dc} Kc further with the license key Kc1 or Kc2 inputted from the switch 1518 in response to enciphered content data {Dc} Kc from bus BS2. When only the license for an audition is being recorded on the memory card 110 it is accepted audition field {Dc1} Kc1 in which decoding reproduction is possible and is refreshable at license key Kc1.

[0096] The portable telephone 100 is provided with the following.

The music reproduction section 1520 for reproducing contents data in response to the output from the decoding processing section 1519.

DA converter 1521 which changes the output of the music reproduction section 1520 into an analog signal from a digital signal.

The terminal 1522 for outputting the output of DA converter 1521 to external output devices (graphic display abbreviation) such as a head telephone.

[0097] In drawing 7 the field enclosed with a dotted line constitutes the contents playback circuit 1550 which decodes enciphered content data and reproduces music data.

[0098] The operation in each session of each component part of the portable telephone 100 will be later explained in detail using a flow chart.

[0099] Drawing 8 is a schematic block diagram for explaining the composition of the memory card 110 shown in drawing 1.

[0100] As already explained as the class public presentation encryption key and class secret decode key of a memory card Kpmw and Kmw are provided and the class certificate Cmw of a memory card is formed but it shall be expressed with the natural number w=3 in the memory card 110. The natural number x which identifies a memory card shall be expressed with x=4.

[0101] Therefore the memory card 110 is provided with the following.

Authentication data {Kpm3//Cm3}. Authentication data attaching part 1400 holding KPa

The Kmc attaching part 1402 holding individual secret decode key Kmc4 which is a peculiar decode key set up for every memory card.

The Km attaching part 1421 holding class secret decode key Km3.

The KPmc attaching part 1416 holding open encryption key KPmc4 which can be decoded by individual secret decode key Kmc4.

[0102] Thus by forming the encryption key of a recorder called a memory card it becomes possible to perform management of the distributed contents data or the enciphered license key per memory card so that it may become clear in the following explanation.

[0103] The memory card 110 is provided with the following.

The interface 1424 which delivers and receives a signal via the terminal 1426 between the memory card interfaces 1200.

Bus BS4 which exchanges a signal between the interfaces 1424.

The decoding processing section 1422 which outputs session key Ks1 which the distributing server 10 generated in the distribution session from the data given to bus BS4 from the interface 1424 from the Km attaching part 1421 in response to the fact that class secret decode key Km3 to contact Pa.

Perform decoding processing by the open authentication key KPa from the data given to bus BS4 in response to the open authentication key KPa from the KPa attaching part 1414 and a decoding result and the obtained class certificate for the controller 1420. The decoding processing section 1408 which outputs the obtained class public key to the enciphering processing part 1410 and the enciphering processing part 1406 which enciphers the data selectively given by the change-over switch 1446 and is outputted to bus BS4 with the key selectively given by the change-over switch 1442.

[0104] The memory card 110 is provided with the following.

Distribution and the session key generating part 1418 which generates session key Ks2 in each reproductive session.

The enciphering processing part 1410 which enciphers session key Ks2 which the session key generating part 1418 outputted with the class public presentation encryption keys KPPy and KPMw obtained by the decoding processing section 1408 and is sent out to bus BS4.

The decoding processing section 1412 decoded by session key Ks2 obtained from the session key generating part 1418 in response to the data enciphered by session key Ks2 from bus BS4.

The cipher-processing part 1417 which enciphers the license key Kc and the reproduction control information ACp which were read from the memory 1415 in the reproduction session of enciphered content data with the individual public presentation encryption key KPMcx of other memory cards 110 decoded by the decoding processing section 1412 (x!=4).

[0105] The decoding processing section 1404 for the memory card 110 to decode the data on bus BS4 further by individual public presentation encryption key KPMc4 and individual secret decode key Kmc4 of the memory card 110 which make a pair. Enciphered content data {Dc} The memory 1415 for storing in response to Kc the license (KcACpACmlicense IDcontent ID) for reproducing enciphered content data {Dc} Kc and additional information Dc-inf from bus BS4 is included. The memory 1415 is constituted by semiconductor memory for example. The memory 1415 comprises the license area 1415A and the data area 1415B. The license area 1415A is a field for recording a license. The data area 1415B is a field for recording enciphered content data {Dc} Kc and additional information Dc-inf of enciphered content data. It

is accessible from the outside in the data area 1415B.

[0106] Further the memory card 110 performs data transfer between the exteriors via bus BS4 and contains the controller 1420 for controlling operation of the memory card 110 in response to reproduction information etc. between bus BS4.

[0107] The license area 1415A is constituted by the Tampa-proof module field. The license area 1415A and the data area 1415B do not need to be constituted in the one memory 1415 and may be constituted independently respectively. The memory 1415 may be a field only for a license without the data area 1415B.

[0108] Hereafter operation of each session in the data distribution system shown in drawing 1 is explained.

[0109] [Distribution for an audition] the distributing server 10 shown in drawing 1 The operation which distributes the license for an audition which contains encrypted-music-data {Dc} Kc and license key Kc1 in the memory card 110 with which the portable telephone 100 was equipped via the portable telephone network and the license for main parts containing license key Kc2 is explained. Drawing 9 is a flow chart of the license for an audition containing encrypted-music-data {Dc} Kc [from the distributing server 10 to the memory card 110] and license key Kc1 and license Kc1 and Kc2 which shows operation by the whole distribution. The portable telephone 100 transmits the distribution request of the license for an audition which contains encrypted-music-data {Dc} Kc and license key Kc1 to the distributing server 10 via a portable telephone network according to directions of the user of the portable telephone 100. Encrypted music data {Dc} from the distributing server 10 Kc and the license for an audition are received. And the portable telephone 100 records the license for an audition containing encrypted-music-data {Dc} Kc and license key Kc1 which received on the memory card 110 (Step S10). Then the portable telephone 100 reads audition field {Dc1} Kc1 and license key Kc1 which are a part of encrypted-music-data {Dc} Kc from the memory card 110 according to the audition directions from a user. Encrypted-music-data {Dc1} Kc1 which can be decoded by license key Kc1 contained in the license for an audition in the contents playback circuit 1550 is decoded and reproduced. And a user tries listening the reproduced music data via the head telephone 130 (Step S20).

[0110] A user inputs into the portable telephone 100 the download request of the license for main parts containing license key Kc2 when you wish the purchase of the music data which it tried listening. If it does so the portable telephone 100 will transmit the distribution request of the license for main parts which contains license key Kc2 via a portable telephone network to the distributing server 10. The license for main parts which contains license key Kc2 from the distributing server 10 is received and the license for main parts containing the license key Kc2 which received is recorded on the memory card 110 (Step S30). Then the portable telephone 100 reads encrypted-music-data {Dc} Kc and two license key Kc1 and Kc2 from the memory card 110 according to a user's reproduction request. In the contents playback circuit 1550 encrypted-music-data {Dc} Kc is decoded and

reproduced using license key Kc1 and license key Kc2 which suited each field of enciphered content data {Dc} Kc.

[0111] Hereafter the details of Step S10, S20 and S30 are explained. Drawing 10 and drawing 11 are the flow charts for explaining detailed operation of the message distribution processing of the license in Step S10 and Step S30 of drawing 9.

First the details of Step S10 which downloads the license for an audition and enciphered content data {Dc} Kc from the distributing server 10 are explained.

[0112] Before the processing in drawing 10 the user of the portable telephone 100 connects via a telephone network to the distributing server 10 and is premised on having acquired the content ID to the contents which wish to purchase and having determined the kind of license to need. The license key Kci (i= 12) in a flow chart is a license key of either Kc1 or Kc2 and since it aims at acquisition of the license for an audition which contains license key Kc1 in this case it is i= 1. Distribution of i= 1 and the license for a reading **** audition is explained for i of the license key Kci in drawing 10 and drawing 11.

[0113] With reference to drawing 10 the distribution request by specification of content ID is made via the navigational panel 1111 from the user of the portable telephone 100 (Step S100). And the terms of purchase AC for purchasing license Kc of encrypted-music-data {Dc1} Kc1 for audition1 via the navigational panel 1111 are inputted (Step S102). That is it is directed whether as conditions for downloading the license key Kci which decodes selected encrypted-music-data {Dc} Kc are license key Kc1 and it is license key Kc2 i.e. the license for an audition and whether it is the license for main parts. In the license for main parts the conditions for setting up the access control information ACm of enciphered content data and the reproduction control information ACp are inputted as the license terms of purchase AC.

[0114] If the terms of purchase AC of enciphered content data are inputted the controller 1109 will give the output instruction of authentication data to the memory card 110 via bus BS2 and the memory card interface 1200 (Step S104). The controller 1420 of the memory card 110 receives the Request to Send of authentication data via the terminal 1426 the interface 1424 and bus BS4 (Step S106). And the controller 1420 reads authentication data {Kp3//Cm3} KPa from the authentication data attaching part 1400 via bus BS4 and outputs {Kp3//Cm3} KPa via bus BS4 the interface 1424 and the terminal 1426 (Step S108).

[0115] In addition to authentication data {Kp3//Cm3} KPa from the memory card 110 the controller 1109 of the portable telephone 100 transmits the data AC and the distribution request of content ID and license terms of purchase to the distributing server 10 (Step S110).

[0116] In the distributing server 10 the distribution request from the portable telephone 100 content ID Authentication data {Kp3//Cm3} The data AC of KPa and license terms of purchase is received (Step S112) and decoding processing is performed for the authentication data outputted from the memory card 110 in the

decoding processing section 312 with the open authentication key KPa (Step S114).
[0117] Authenticating processing which judges whether the distribution control part 315 received the authentication data enciphered for proving the justification in a regular organization from the decoding processing result in the decoding processing section 312 is performed (Step S116). When it is judged that it is just authentication data the distribution control part 315 recognizes and receives class public presentation encryption key KPm3 and class certificate Cm3. And it shifts to the next processing (Step S118). In not being just authentication data it is considered as non approval and it ends a distribution session without receiving class public presentation encryption key KPm3 and class certificate Cm3 (Step S164).

[0118] If it is checked that it is access from the portable telephone which equipped with the memory card with just authentication data as a result of attestation in the distributing server 10 the session key generating part 316 will generate session key Ks1 for distribution (Step S118). Session key Ks1 is enciphered by the enciphering processing part 318 by class public presentation encryption key KPm3 corresponding to the memory card 110 obtained by the decoding processing section 312 (Step S120).

[0119] The distribution control part 315 generates license ID (Step S122) and license ID and session key Ks1 which were enciphered are outputted outside via bus BS1 and the communication apparatus 350 as license ID//[Ks1] Km3 (Step S124).

[0120] If the portable telephone 100 receives license ID//[Ks1] Km3 the controller 1109 will input license ID//[Ks1] Km3 into the memory card 110 (Step S126). If it does so in the memory card 110 the controller 1420 will receive license ID//[Ks1] Km3 via the terminal 1426 and the interface 1424 (Step S128). And give the controller 1420 to the decoding processing section 1422 via bus BS4 and [Ks1] Km3 the decoding processing section 1422 By carrying out decoding processing by class secret decode key Km3 [peculiar to the memory card 110 held at the attaching part 1421] session key Ks1 is decoded and session key Ks1 is received (Step S132).

[0121] The controller 1420 directs generation of session key Ks2 generated in the memory card 110 to the session key generating part 1418 at the time of distribution operation if acceptance of session key Ks1 generated with the distributing server 10 is checked. And the session key generating part 1418 generates session key Ks2 (Step S134).

[0122] The enciphering processing part 1406 by session key Ks1 given from the decoding processing section 1422 via contact Pa of the change-over switch 1442. Session key Ks2 given by switching the point of contact of the change-over switch 1446 one by one and individual public presentation encryption key KPmc4 are enciphered as one data row and [Ks2//KPmc4] Ks1 is outputted to bus BS4. Encryption data [Ks2//KPmc4] Ks1 outputted to bus BS4 is outputted to the portable telephone 100 via the interface 1424 and the terminal 1426 from bus BS4 (Step S138) and it is transmitted to the distributing server 10 from the portable telephone 100 (Step S140).

[0123]With reference to drawing 11the distributing server 10 receives {Ks2//KPmc4} Ks1In the decoding processing section 320decoding processing by session key Ks1 is performedand session key Ks2 generated with the memory card 110 and open encryption key KPmc4 [peculiar to the memory card 110] are received (Step S142).

[0124]The distribution control part 315 acquires license key Kc1 from the information database 304 according to the content ID and the terms of purchase AC which were acquired at Step S112 (Step S144)According to the data AC of the license terms of purchase acquired at Step S112the access control information ACm and the reproduction control information ACp are determined (Step S146).

[0125]The distribution control part 315 gives the generated licensei.e.license IDcontent IDlicense key Kcthe reproduction control information ACpand the access control information ACm to the enciphering processing part 326. By open encryption key KPmc4 [peculiar to the memory card 110 obtained by the decoding processing section 320]the enciphering processing part 326 enciphers a license and generates encryption data {license ID// content ID//Kc1//ACm//ACp} Kmc4 (Step S148). And the enciphering processing part 328 encryption data {license ID// content ID//Kc1//ACm//ACp} Kmc4 from the enciphering processing part 326It enciphers by session key Ks2 from the decoding processing section 320and encryption data {{license ID// content ID//Kc1//ACm//ACp} Kmc4} Ks2 is outputted. The distribution control part 315 transmits encryption data {{license ID// content ID//Kc1//ACm//ACp} Kmc4} Ks2 to the portable telephone 100 via bus BS1 and the communication apparatus 350 (Step S150).

[0126]The portable telephone 100 receives encryption data {{license ID// content ID//Kc1//ACm//ACp} Kmc4} Ks2 transmittedand inputs it into the memory card 110 via bus BS2 (Step S152). In the memory card 110the received data given to bus BS4 are decoded by the decoding processing section 1412 via the terminal 1426 and the interface 1424. The decoding processing section 1412 decodes the received data of bus BS4 using session key Ks2 given from the session key generating part 1418and outputs them to bus BS4 (Step S154).

[0127]In this stageencryption license {license ID// content ID//Kc1//ACm//ACp} Kmc4 which can be decoded by secret decode key Kmc4 held at the Kmc attaching part 1402 is outputted to bus BS4 (Step S154).

[0128]With directions of the controller 1420encryption license {license ID// content ID//Kc1//ACm//ACp} Kmc4In the decoding processing section 1404it is decoded by individual secret decode key Kmc4and a license (license key Kc1license IDcontent IDthe access control information ACmand reproduction control information ACp) is received (Step S156).

[0129]If it does sothe controller 1420 of the memory card 110 stores the received license (license IDcontent IDlicense key Kc1the access control information ACmand reproduction control information ACp) in the license area 1415A (Step S160). And accounting is performed in the distributing server 10. That isthe distribution control part 315 records accounting information on the charge database 302 (Step S162).

The charging cost to distribution of the license for an audition in this case is lower than the charging cost to distribution of the license for main parts mentioned later. And distribution operation of a license is ended (Step S164).

[0130] Enciphered content data {Dc} about Kc. Since it is mere download processing, do not explain to details but after distribution operation of the license for an audition is completed, the controller 1109 of the portable telephone 100 transmits the distribution request of enciphered content data to the distributing server 10. The distributing server 10 receives the distribution request of enciphered content data. And from the information database 304, the distribution control part 315 of the distributing server 10 acquires enciphered content data {Dc} Kc and additional information Dc-inf and outputs these data via bus BS1 and the communication apparatus 350.

[0131] The portable telephone 100 receives {Dc} Kc//Dc-inf and receives enciphered content data {Dc} Kc and additional information Dc-inf. If it does so, the controller 1106 will input enciphered content data {Dc} Kc and additional information Dc-inf into the memory card 110 via bus BS2 and the memory card interface 1200. The controller 1420 of the memory card 110 records enciphered content data {Dc} Kc and additional information Dc-inf which were received on the data area 1415B of the memory 1415. The license for changing the license key in which it is shown which block should be decoded with which license key among enciphered content data {Dc} Kc(s) and the matching information of a block are included in additional information Dc-inf.

[0132] Thus, in distribution of a license, the memory card 110 with which the portable telephone 100 was equipped is apparatus holding regular authentication data. After checking that open encryption key KPm3 which has enciphered and transmitted with class certificate Cm3 is effective simultaneously, contents data can be distributed and distribution of the contents data to an inaccurate memory card can be forbidden.

[0133] By exchanging the encryption key generated with a distributing server and a memory card respectively, performing encryption using the encryption key which each received and transmitting the encryption data to the other party, De facto mutual recognition can be performed also in transmission and reception of each encryption data and the security of a data distribution system can be raised.

[0134] Although it explained in the above having charged to distribution of the license for an audition (Step S162), an audition is service aiming at having the license for main parts downloaded and since I need to get more users to hear it, not charging to distribution of the license for an audition is also possible.

[0135] [Audition] Next, the audition in Step S20 is explained in detail. In the reproduction for an audition, the controller 1109 of the portable telephone 100 attaches data Dc-inf of the musical piece which performs reproduction is read from MEMOKADO 110. One new enciphered content data which specifies the block which constitutes refreshable field {Dc1} Kc1 for an audition from a license for an audition and comprises only a specified block is generated virtually and this

enciphered content data generated virtually is decoded and it reproduces. With reference to (a) of drawing 3 when enciphered content data {Dc} Kc is the enciphered content data 90 the data row which checks the block which constitutes the audition field 91 ({Dc1} Kc1) and comprises only an applicable block is reproduced as one musical piece. With reference to (b) of drawing 3 when enciphered content data {Dc} Kc is the enciphered content data 93 the audition field 94 ({Dc1} Kc1) is similarly reproduced as one musical piece.

[0136] "Reproduction consent" which reproduction makes license key Kc1 first contained in the license for an audition stored in the memory card 110 hold to either of the two Kc attaching parts 1514-1515 in the contents playback circuit 1550. After "reproduction consent" license key Kc1 currently held at either of the Kc attaching parts 1514-1515 is chosen with the switch 1518 and the decoding processing section 1519 is supplied. The enciphered content data virtually constituted for the audition corresponds with field {Dc1} Kc1 for an audition. Therefore enciphered content data {Dc1} Kc1 shall express the enciphered content data virtually constituted for the audition.

[0137] If it does so the controller 1109 will read the block which constitutes enciphered content data {Dc1} Kc1 from the memory card 110 according to reproduction sequence and will supply it to the decoding processing section 1519. The decoding processing section 1519 the block which constitutes the inputted enciphered content data by license key Kc1. The plaintext-sized block (block which constitutes source data) which constitutes the contents data produced by decoding respectively and decoding enciphered content data {Dc1} Kc1 is extracted. And the decoding processing section 1519 outputs the extracted block to the music reproduction section 1520. Based on the data contained in the block supplied from the decoding processing section 1519 the music reproduction section 1520 carries out digital playback of the music and supplies it to A/D converter 1521. If it does so A/D converter 1521 will change contents data into an analog signal from a digital signal and will output it to the terminal 1522. And all the blocks which constitute enciphered content data {Dc1} Kc1 are read from the memory card 110 to reproduction orders and after a series of processings are completed the reproduction for an audition is completed. The user can try listening audition field {Dc1} Kc1 of this enciphered content data {Dc} Kc by the head telephone 130 grade connected to the terminal 1522.

[0138] After a series of processings to all the blocks which are the reproductive targets were completed at this time explained that the reproduction for an audition was completed but. After read-out of all the blocks which are the reproductive targets on the assumption that a repetition audition is carried out is completed it is also possible to constitute so that it may return and reproduce continuously to the block of the head of enciphered content data {Dc1} Kc1. In this case a user operates the navigational panel 1111 the end of an audition points to the end of an audition for the controller 1109 and the controller 1109 constitutes it so that reproduction may

be ended according to directions.

[0139] Next reproduction consent which makes license key Kc1 contained in the license for an audition hold to either of the two Kc attaching parts 1514-1515 in the contents playback circuit 1550 is explained. Drawing 12 is a flow chart for explaining operation of "reproduction consent." "Reproduction consent" not only making license key Kc1 of the license for an audition hold to either of the Kc attaching parts 1514-1515 but it is also the processing which makes license key Kc2 of the license for main parts hold to either of the Kc attaching parts 1514-1515 and Kci [a license key] is written in drawing 12. The identifier i which distinguishes a license key in an audition performs i= 1 and reading **** explanation. License key Kc1 explains as what is held at the Kc attaching part 1514.

[0140] If the reproduction motion for an audition is started with reference to drawing 12a reproduction consent request will be inputted to the portable telephone 100 via the navigational panel 1111 from the user of the portable telephone 100 (Step S200). If it does so the controller 1109 will perform the output requirement of authentication data in the contents playback circuit 1550 via bus BS2 (Step S202) and the contents playback circuit 1550 will receive the output requirement of authentication data (Step S204). And the authentication data attaching part 1500 outputs authentication data {Kp1//Cp1} KPa (Step S206) and the controller 1109 authentication data {Kp1//Cp1} KPa is inputted into the memory card 110 via the memory card interface 1200 (Step S208).

[0141] When it does so the memory card 110 receives authentication data {Kp1//Cp1} KPa and the decoding processing section 1408 received authentication data {Kp1//Cp1} Decoding KPa with the open authentication key KPa held at the KPa attaching part 1414 (Step S210) the controller 1420 performs authenticating processing from the decoding processing result in the decoding processing section 1408. That is authentication data {Kp1//Cp1} KPa performs authenticating processing which judges whether it is regular authentication data (Step S212). When it is not able to decode it shifts to Step S260 and reproduction motion is ended. When authentication data is able to be decoded the controller 1420 controls the session key generating part 1418 and the session key generating part 1418 generates session key Ks2 for reproduction sessions (Step S214). And the cipher-processing part 1410 outputs {Ks2} Kp1 which enciphered session key Ks2 from the session key generating part 1418 by open encryption key Kp1 decoded by the decoding processing section 1408 to bus BS4. If it does so the controller 1420 will output {Ks2} Kp1 to the memory card interface 1200 via the interface 1424 and the terminal 1426 (Step S216). The controller 1109 of the portable telephone 100 acquires {Ks2} Kp1 via the memory card interface 1200. And the controller 1109 gives {Ks2} Kp1 to the decoding processing section 1504 of the contents playback circuit 1550 via bus BS2 (Step S218) By secret decode key Kp1 which was outputted from the Kp1 attaching part 1502 and which is open encryption key Kp1 and a pair the decoding processing section 1504 decodes {Ks2} Kp1 and outputs session key Ks2 to the cipher-

processing part 1506 (Step S220). If it does so the session key generating part 1508 will generate session key Ks3 for reproduction sessions and will output session key Ks3 to the cipher-processing part 1506 (Step S222). The cipher-processing part 1506 enciphers session key Ks3 from the session key generating part 1508 by session key Ks2 from the decoding processing section 1504 and outputs {Ks3} Ks2 (Step S224). The controller 1109 outputs {Ks3} Ks2 to the memory card 110 via bus BS2 and the memory card interface 1200 (Step S226).

[0142] If it does so the decoding processing section 1412 of the memory card 110 will input {Ks3} Ks2 via the terminal 1426, the interface 1424 and bus BS4. The decoding processing section 1412 decodes {Ks3} Ks2 by session key Ks2 generated by the session key generating part 1418 and receives session key Ks3 generated with the reproduction terminal 100 (Step S228).

[0143] The controller 1109 of the portable telephone 100 The entry number in which the license is stored is acquired from the license management file of the reproduction request song beforehand acquired from the memory card 110 (Step S230). The output requirement of the entry number acquired to the memory card 110 via the memory card interface 1200 and a license is outputted (Step S232).

[0144] The controller 1420 of the memory card 110 receives an entry number and the output requirement of a license and acquires the license stored in the field specified with the entry number (Step S234).

[0145] And the controller 1420 checks the access restriction information ACm (Step S236).

[0146] In Step S236 by checking the access restriction information ACm which is information about the restriction to access of a memory specifically By checking reproduction frequency it ends reproduction motion in being in a state [that it is already unreproducible] and it progresses to the following step (Step S240) after changing the reproduction frequency of the access restriction information ACm (Step S238) when the reproduction frequency of access restriction information has restriction. On the other hand when reproduction is not restricted by the reproduction frequency of the access restriction information ACm Step S238 is skipped and processing advances to the following step (Step S240) without changing the reproduction frequency of the access restriction information ACm.

[0147] In Step S236 when it is judged that it is renewable in the reproduction motion concerned license key Kc1 of a reproduction request song and the reproduction control information ACp which were recorded on the license area 1415A of the memory 1415 are outputted on bus BS4 (Step S240).

[0148] The license key Kc and the reproduction control information ACp which were acquired are sent to the enciphering processing part 1406 via the point of contact Pf of the change-over switch 1446. The enciphering processing part 1406 enciphers license key Kc1 and the reproduction control information ACp which were received via the change-over switch 1446 by session key Ks3 received from the decoding processing section 1412 via the point of contact Pb of the change-over switch

1442[Kc1//ACp] Ks3 is outputted to bus BS4 (Step S240).

[0149]The encryption data outputted to bus BS4 is sent out to the reproduction terminal 102 via the interface 1424the terminal 1426and the memory card interface 1200.

[0150]In the portable telephone 100the decoding processing section 1510 performs decoding processing for encryption data [Kc//] {ACp} Ks3 transmitted to bus BS2 via the memory card interface 1200The license key Kc and the reproduction control information ACp are received (Step S242S244). The decoding processing section 1510 outputs the license key Kc (in this case license key Kc1) to the switch 1511.

[0151]The decoding processing section 1510 outputs the reproduction control information ACp to bus BS2. Via bus BS2the controller 1109 receives the reproduction control information ACpand checks reproductive propriety (Step S246).

[0152]In Step S246when it is judged by the reproduction control information ACp that reproduction is impossibleit points on the switch 1511 so that the license key Kci may be outputted to the terminal 1512and the Kc attaching part 1514 holds the license key Kci.

[0153]Thusafter license key Kc1 is held at the Kc attaching part 1415 and processing of "reproduction consent" is completedenciphered content data {Dc1} Kc1 becomes refreshable. On the other handit branches by Step S212S236and S246and after license key Kc1 is completed [that as is held "reproduction consent" and] to the Kc attaching part 1415enciphered content data {Dc1} Kc1 is unreplicable.

[0154]Thereforeit has composition which cannot reproduce the user who does not possess a regular license even if it is reproduction of only audition field {Dc1} Kc1 which is a part of enciphered content data {Dc} Kc even if. Of courseenciphered content data {Dc} Kc may be acquired by a certain meansand the acquired enciphered content data {Dc} Kc may be copied. If the license for an audition is acquired from the distributing server 10it is refreshable in enciphered content data {Dc} Kc.

[0155]Since only the license for an audition is held in an auditionunless the license for main parts is acquiredthe block outside the audition field enciphered as decoding in license key Kc2i.e.body area {Dc2} Kc2is unreplicable.

[0156][Distribution of the license for main parts] Nextdownload of the license for main parts in Step S30 is explained in detail. Download of the license for main parts is processed like the processing in download of the license for an audition according to the flow chart of drawing 10 and drawing 11. In this casesince it is download of the license containing license key Kc2the information which shows that it is the purchase of the license for main parts is included in the license terms of purchase AC. Since reading ***** is good for Kc2 and explanation overlaps the identifier i which distinguishes the license key in a flow chart in i= 2 [Kci]i.e.a license keyexplanation is omitted.

[0157]Hereeven after acquiring the license for main partsexplained that it

reproduced using the license for an audition containing license key Kc1 to reproduction of enciphered content databut. After using for the license for an audition the reproduction frequency restrictions included in the access control information ACmfor exampleadding about three number-of-times restrictionsThe same service can be providedeven if it distributes gratuitously and distributes simultaneously two licensesi.e.the license containing license key Kc1and the license containing license key Kc2 as a license for main parts. In this casethe portable telephone 100 receives distribution of two licenses in Step S30 of drawing 9. That is the flow chart shown in drawing 10 and drawing 11 is acquirable by processing twice.

[0158][Reproduction] After downloading the license for main parts and storing two licenses in the memory card 110 by Step S30the processing which uses two license key Kc1 and Kc2 and reproduces enciphered content data {Dc} Kc is explained. Herein order to explain simplyit explains as that by which license key Kc1 is held at the Kc attaching part 1514and license key Kc2 is held at the license attaching part 1515but it may not be limited to this and may be reverse.

[0159]With reference to drawing 3the case where the enciphered content data 90 is reproduced is explained. The controller 1109 specifies the block which belongs to the field 91 for an audition in the enciphered content data 90and the block belonging to the field 92 for main parts with reference to additional information Dc-inf to the enciphered content data 90.

[0160]Nextreproduction consentfor holding license key Kc2 [required in order to reproduce the first block according to reproduction sequence] to the Kc attaching part 1515 is performed according to the flow chart of drawing 12. In this casesince reading ***** is [identifier / i / which distinguishes the license key in the flow chart of drawing 12] good for Kc2 in $i = 2$ [Kci]i.e.a license keyand it is the same as that of "reproduction consent" in audition reproductionexplanation is omitted.

[0161]Thenchoose the terminal 1517 to the switch 1518and it points so that license key Kc2 currently held at the Kc attaching part 1515 may be outputtedThe block which constitutes the enciphered content data 90 is read from the memory card 110 according to reproduction ordersand the decoding processing section 1519 is supplied. The controller 1109 supplying the block which constitutes the enciphered content data 90 to the decoding processing section 1519 so that reproduction of contents data may be performed continuously. Using the idle time of the processingreproduction consentwhich makes license key Kc1 which is another license key hold to the Kc attaching part 1514 is performedbefore starting supply of the block belonging to the field 91 for an audition. Since it is the same as that of "reproduction consent" in the case of performing reproduction in an auditionreproduction consentto license key Kc1 omits explanation.

[0162]If it does sothe controller 1109 will read the block which constitutes the enciphered content data 90 from the memory card 110It points so that license key Kc1 which chooses the terminal 1516 to the switch 1518 and is held at the Kc

attaching part 1514 may be outputted to the decoding processing section 1519 if reproduction orders are supplied and the field 91 for an audition is arrived at. Then the block which constitutes the enciphered content data 90 is read from the memory card 110 according to reproduction orders and the decoding processing section 1519 is supplied.

[0163] And it points so that license key Kc2 which chooses the terminal 1517 to the switch 1518 again and is held at the Kc attaching part 1515 may be outputted to the decoding processing section 1519 if the field 92 for main parts is arrived at again. Then the block which constitutes the enciphered content data 90 is read from the memory card 110 according to reproduction orders and the decoding processing section 1519 is supplied. Supply of all the blocks will terminate reproduction of the enciphered content data 90.

[0164] With reference to drawing 3 the case where the enciphered content data 93 is reproduced is explained. In the enciphered content data 93 if reproduction orders are followed the field 94 for an audition first reproduced by license key Kc1 exists. Therefore reproduction consent which makes license key Kc1 hold to the Kc attaching part 1514 is performed first. Subsequently the controller 1109 reads the block which constitutes the enciphered content data 93 from the memory card 110 and supplies it to reproduction orders at the decoding processing section 1519. The controller 1109 supplying the block which constitutes the enciphered content data 93 to the decoding processing section 1519 so that reproduction of contents data may be performed continuously. Using the idle time of the processing reproduction consent which makes license key Kc2 which is another license key hold to the Kc attaching part 1515 is performed before starting supply of the block belonging to the field 95 for main parts.

[0165] It points so that license key Kc2 which chooses the terminal 1517 and is held at the Kc attaching part 1514 may be outputted to the decoding processing section 1519 to the switch 1518 if the field 95 for main parts is arrived at. Then the block which constitutes the enciphered content data 93 is read from the memory card 110 according to reproduction orders and the decoding processing section 1519 is supplied. Supply of all the blocks will terminate reproduction of the enciphered content data 93.

[0166] The personal computer 50 shown in drawing 1 can acquire only encrypted-music-data {Dc} Kc from the distributing server 10 or CD-ROM 60 and it can also store in the memory card 110 via the card writer 80. In this case the download processing of the enciphered content data in Step S10 of drawing 9 is omitted.

[0167] The personal computer 50 shown in drawing 1 The license for an audition containing encrypted-music-data {Dc1} Kc1 for an audition encrypted-music-data {Dc2} Kc2 for main parts and license key Kc1 can be acquired from the distributing server 10 or CD-ROM 60 and it can store in the memory card 110 via the card writer 80. In this case the personal computer 50 performs Step S10 of drawing 9 and storing of the license to the memory card 110 which passed the card writer 80 from the

personal computer 50 is performed according to the flow chart shown in drawing 10 and drawing 11. In this case the personal computer 50 achieves the function of the distributing server 10 in drawing 10 and drawing 11 and the portable telephone 100. And the user of the portable telephone 100 extracts the memory card 110 from the card writer 80 and equips the portable telephone 100 and tries listening audition field [Dc1] Kc1 of encrypted-music-data [Dc] Kc according to the flow chart shown in drawing 12. Then license key Kc2 for decoding encrypted-music-data [Dc2] Kc2 for main parts is downloaded according to the flow chart shown in drawing 10 and drawing 11 from the distributing server 10 with the portable telephone 100 to hear encrypted-music-data [Dc] Kc. And the portable telephone 100 reproduces all the encrypted-music-data [Dc] Kc(s) using two license key Kc1 and Kc2 according to a user's reproduction request. Although explained and omitted as for record of acquisition of the license for an audition or the license for an audition to CD-ROM 60 and read-out of the license for an audition, safety shall be secured from the distributing server 10 using encoding technology. However, it shall not limit for the method here. It is also possible for the computer 50 to receive the license for main parts from the distributing server 10 and to store in the memory card 110 via the card writer 80.

[0168] Thus the portable telephone 100 receives two licenses which contain encrypted-music-data [Dc] Kc and license key Kc1 and Kc2 from various kinds of courses respectively and records them on the memory card 110. Therefore when the user of the portable telephone 100 wishes download in the state where all the encrypted-music-data [Dc] Kc(s) are renewable to the memory card 110. Eventually two licenses which contain encrypted-music-data [Dc] Kc and license key Kc1 and Kc2 respectively are stored.

[0169] Although the case where enciphered content data was the enciphered content data which enciphered music data was explained in the above, download of enciphered content data, audition, preview and reproduction are performed by the method mentioned above even if enciphered content data was other reading data, teaching-materials data, a video data etc.

[0170] Since two or more licenses for decoding the enciphered content data divided into two or more blocks and the encryption data contained in two or more blocks are distributed according to the embodiment of the invention, each block can be decoded and reproduced according to a different license. As a result, a charging cost can be set up according to the license distributed.

[0171] With all the points, the embodiment indicated this time is illustration and should be considered not to be restrictive. The range of this invention is shown by the above-mentioned not explanation but claim of an embodiment and it is meant that all the change in a claim is an equivalent meaning and within the limits is included.

[0172]

[Effect of the Invention] According to this invention, since two or more licenses for decoding the enciphered content data divided into two or more blocks and the encryption data contained in two or more blocks are distributed, each block can be

decoded and reproduced according to a different license.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is a schematic diagram which illustrates a data distribution system notionally.

[Drawing 2] It is a figure showing the characteristics such as data for the communication in the data distribution system shown in drawing 1 and information.

[Drawing 3] It is a figure showing the format of enciphered content data.

[Drawing 4] It is a figure for explaining the generation method of enciphered content data.

[Drawing 5] It is a figure showing the characteristics such as data for the communication in the data distribution system shown in drawing 1 and information.

[Drawing 6] It is a schematic block diagram showing the composition of the distributing server in the data distribution system shown in drawing 1.

[Drawing 7] It is a schematic block diagram showing the composition of the portable telephone in the data distribution system shown in drawing 1.

[Drawing 8] It is a schematic block diagram showing the composition of the memory card in the data distribution system shown in drawing 1.

[Drawing 9] It is a flow chart for explaining the entire configuration of the distribution operation in the data distribution system shown in drawing 1.

[Drawing 10] It is the 1st flow chart for explaining distribution operation of the license shown in drawing 9 still in detail.

[Drawing 11] It is the 2nd flow chart for explaining distribution operation of the license shown in drawing 9 still in detail.

[Drawing 12] It is a flow chart for explaining read-out of the license key in reproduction consent operation in detail.

[Drawing 13] It is a figure showing another format of enciphered content data.

[Description of Notations]

10 A distributing server and 20 A distribution carrier
30 Internet networks
50 A personal computer
60 CD
70 USB cables
84 90 93 96 97 enciphered content data and
81 Source data
82 Block data
83 91 92 and 94 and 95 84 28 44 84 6 encrypted music data
100 Portable telephone
110 A memory card and
130 A head telephone
302 charge databases
304 An information database and
307 A menu database and
308 Distribution recording data base
310 A data processing part and
312 320 140 414 081 412 142 215 041 510 and 1519
Decoding processing section
313 An authentication key attaching part and
315 A distribution control part and
316–1418 and 1508 Session key generating part
318 326 328 140 614 101 417 and 1506 Cipher-processing part
350 A communication apparatus and
841 and 843 845 971 972 Encryption data
961–967 [A transmission and reception section and
1103 /

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-288376

(P2002-288376A)

(43) 公開日 平成14年10月4日 (2002.10.4)

(51) Int.Cl.⁷

G 0 6 F 17/60

識別記号

1 4 2

Z E C

3 0 2

5 1 2

F I

G 0 6 F 17/60

テ-マ-ト* (参考)

1 4 2

Z E C

3 0 2 E

5 1 2

審査請求 未請求 請求項の数13 O L (全 25 頁)

(21) 出願番号 特願2001-87300(P2001-87300)

(22) 出願日 平成13年3月26日 (2001.3.26)

(71) 出願人 000001889

三洋電機株式会社

大阪府守口市京阪本通2丁目5番5号

(72) 発明者 堀 吉宏

大阪府守口市京阪本通2丁目5番5号 三洋電機株式会社内

(72) 発明者 日置 敏昭

大阪府守口市京阪本通2丁目5番5号 三洋電機株式会社内

(74) 代理人 100064746

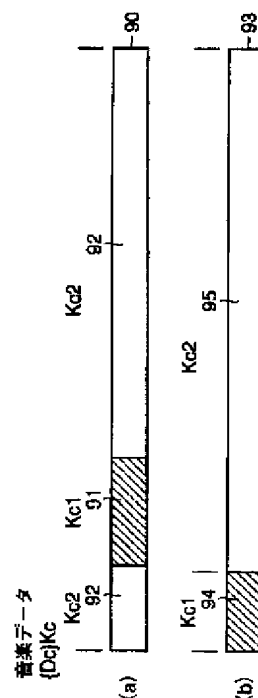
弁理士 深見 久郎 (外3名)

(54) 【発明の名称】 コンテンツ提供方法、データ再生装置、およびデータ記録装置

(57) 【要約】

【課題】 複数のブロックに分離された暗号化コンテンツデータと、複数のブロックに含まれる暗号化データを復号および再生するための複数のライセンスとを配信するコンテンツ提供方法を提供する。

【解決手段】 音楽データを暗号化した暗号化コンテンツデータ90または93は、試験用の暗号化音楽データ91または94と本体用の暗号化音楽データ92または95から成る。暗号化音楽データ91、94はライセンス鍵Kc1によって復号され、暗号化音楽データ92、95はライセンス鍵Kc2によって復号される。配信サーバは、暗号化コンテンツデータ90、93およびライセンス鍵Kc1、Kc2を保持しており、配信要求に応じて試験用の暗号化音楽データ91または94およびライセンス鍵Kc1、本体用の暗号化音楽データ92または95およびライセンス鍵Kc2の順序で配信する。



【特許請求の範囲】

【請求項1】 コンテンツデータを暗号化した暗号化コンテンツデータの取得要求を受信する第1のステップと、

前記第1のステップにおいて受信した取得要求に応じて、前記暗号化コンテンツデータを提供する第2のステップと、

前記暗号化コンテンツデータの一部に対応し、かつ、前記一部を復号するための第1のライセンスの提供要求を受信する第3のステップと、

前記第3のステップにおいて受信した提供要求に応じて、前記第1のライセンスを提供する第4のステップと、

前記第1のライセンスと異なり、かつ、前記暗号化コンテンツデータの前記第1のライセンスに対応しない他の一部に対応し、前記他の一部を復号するための第2のライセンスの提供要求を受信する第5のステップと、

前記第5のステップにおいて受信した提供要求に応じて、前記第2のライセンスを提供する第6のステップと、

前記第2のライセンスの提供に対して課金処理を行なう第7のステップとを含むコンテンツ提供方法。

【請求項2】 前記暗号化コンテンツデータ、前記第1のライセンス、および前記第2のライセンスが同じサーバから配信される、請求項1に記載のコンテンツ提供方法。

【請求項3】 前記暗号化コンテンツデータ、および前記第1のライセンスが第1のサーバから配信され、前記第2のライセンスが前記第1のサーバと異なる第2のサーバから配信される、請求項1に記載のコンテンツ提供方法。

【請求項4】 前記暗号化コンテンツデータ、および前記第1のライセンスは、記録媒体を介して前記第1のサーバに供給される、請求項3に記載のコンテンツ提供方法。

【請求項5】 前記暗号化コンテンツデータが第1のサーバから提供され、前記第1および第2のライセンスが前記第1のサーバと異なる第2のサーバから配信される、請求項1に記載のコンテンツ提供方法。

【請求項6】 前記暗号化コンテンツデータは、記録媒体を介して前記第1のサーバに供給される、請求項5に記載のコンテンツ提供方法。

【請求項7】 前記第3のステップにおいて、前記提供要求とともに認証データを受信し、前記認証データが認証されると前記第1のライセンスを提供し、前記第5のステップにおいて、前記提供要求とともに認証データを受信し、前記認証データが認証されると前記第2のライセンスを提供する、請求項1から請求項6のいずれか1項に記載のコンテンツ提供方法。

【請求項8】 複数のブロックから成る暗号化コンテンツデータを前記複数のブロックに対応する複数のライセンスによって復号して再生するデータ再生装置であって、

前記暗号化コンテンツデータ、および前記複数のライセンスが記録されたデータ記録装置とのやり取りを行なうインタフェースと、

指示を入力するための操作部と、

前記暗号化コンテンツデータを前記複数のライセンスによって復号して再生するコンテンツ再生部と、

制御部とを備え、

前記制御部は、前記コンテンツ再生部において、前記暗号化コンテンツデータを構成する n 番目(n は自然数)のブロックに含まれる暗号化データが前記 n 番目のブロックに対応する n 番目のライセンスによって復号および再生されているときに、 $n+1$ 番目のライセンスを前記インタフェースを介して前記データ記録装置から取得して前記コンテンツ再生部に与える、データ再生装置。

【請求項9】 前記コンテンツ再生部は、前記 n 番目のライセンスに含まれる n 番目のライセンス鍵を保持する第1のライセンス鍵保持部と、

前記 $n+1$ 番目のライセンスに含まれる $n+1$ 番目のライセンス鍵を保持する第2のライセンス鍵保持部と、

前記第1および第2のライセンス鍵保持部から前記 n 番目のライセンス鍵と前記 $n+1$ 番目のライセンス鍵とを選択的に取得し、その取得したライセンス鍵によって対応する暗号化データを復号する復号部と、

前記復号部によって復号されたコンテンツデータを再生する再生部とを含む、請求項8に記載のデータ再生装置。

【請求項10】 前記制御部は、鍵変更情報を前記インタフェースを介して前記データ記録装置から取得し、前記鍵変更情報に基づいて前記 n 番目のライセンス鍵と前記 $n+1$ 番目のライセンス鍵とを選択して前記復号部に与える、請求項9に記載のデータ再生装置。

【請求項11】 前記データ記録装置から前記複数のライセンスの各々を取得するセッションにおいて、異なるセッションキーを発生するセッションキー発生部と、前記セッションキー発生部によって発生されたセッションキーを受け、そのセッションキーによって暗号化ライセンス鍵を復号し、その復号したライセンス鍵を前記第1または第2のライセンス鍵保持部に与えるライセンス鍵復号部とをさらに備え、

前記制御部は、前記セッションキー発生部によって発生されたセッションキーを前記インタフェースを介して前記データ記録装置に入力し、前記セッションキーによって暗号化された暗号化ライセンス鍵を前記インタフェースを介して前記データ記録装置から取得して前記ライセンス鍵復号部に与える、請求項10に記載のデータ再生装置。

【請求項12】 前記ライセンス鍵を提供するライセンス配信サーバから前記ライセンス鍵をダウンロードするための通信を行なうデータ送受信部をさらに備え、前記制御部は、前記暗号化コンテンツデータの全部を再生するために必要なライセンスが前記データ記録装置に記録されていないとき、前記データ記録装置に格納されている前記暗号化コンテンツデータに対応する前記複数のライセンスによって再生可能なブロックのみを前記暗号化コンテンツデータの再生順に従って、前記データ記録装置から取得して前記コンテンツ再生部に与え、前記操作部から入力される新たなライセンス鍵の取得指示に従って前記ライセンス配信サーバから前記暗号化コンテンツデータを構成するブロックに対応するライセンス鍵を前記データ送受信部を介して受信し、その受信したライセンス鍵を前記データ記録装置に記録する、請求項8に記載のデータ再生装置。

【請求項13】 複数のブロックから成る暗号化コンテンツデータおよび前記複数のブロックに含まれる複数の暗号化データを復号するための複数のライセンスとを記録するデータ記録装置であって、前記複数のライセンスを格納するライセンス領域と、前記暗号化コンテンツデータと、前記複数のライセンスの各々と前記暗号化コンテンツデータを構成する前記複数のブロックとの対応を示すライセンス対応情報とを格納するデータ領域とを備えるデータ記録装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は、コピーされた情報に対する著作権保護を可能とするデータ配信システムにおけるコンテンツ提供方法、データ再生装置、およびデータ記録装置に関するものである。

【0002】

【従来の技術】 近年、インターネット等のデジタル情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【0003】 このようなデジタル情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

【0004】 したがって、このようなデジタル情報通信網上において音楽データや画像データ等の著作権者の権利が存在するコンテンツデータが伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【0005】 一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介してコンテンツデー

タの配信を行なうことができないとすると、基本的には、コンテンツデータの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【0006】 ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタルデータを記録した記録媒体を例にとって考えて見ると、通常販売されている音楽データを記録したCD（コンパクトディスク）については、CDから光磁気ディスク（MD等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やMD等の媒体の代金のうちの一定額を間接的に著作権者に対して保証金として支払うことになっている。

【0007】 しかも、CDからMDへデジタル信号である音楽データをコピーした場合、これらの情報がコピー劣化の殆どないデジタルデータであることに鑑み、記録可能なMDからさらに他のMDに音楽情報をデジタルデータとしてコピーすることは、著作権保護のために機器の構成上できないようになっている。

【0008】 このような事情からも、音楽データや画像データをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

【0009】 この場合、デジタル情報通信網を通じて公衆に送信される著作物である音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

【0010】 そこで、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバが、携帯電話機等の端末装置に装着されたメモリカードに対して端末装置を介して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカードの公開暗号鍵とその証明書を暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、配信サーバが認証された証明書を受信したことを確認した上でメモリカードに対して暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンス鍵を送信する。そして、暗号化コンテンツデータやライセンス鍵を配信する際、配信サーバおよびメモリカードは、配信毎に異なるセッションキーを発生させ、その発生させたセッションキーによって公開暗号鍵の暗号化を行ない、配信サーバ、メモリカード相互間で鍵の交換を行なう。

【0011】 最終的に、配信サーバは、メモリカード個々の公開暗号鍵によって暗号化され、さらにセッションキーによって暗号化したライセンスと、暗号化コンテン

ツデータとをメモリカードに送信する。そして、メモリカードは、受信したライセンスと暗号化コンテンツデータとを記録する。

【0012】そして、メモリカードに記録された暗号化コンテンツデータを再生するときは、メモリカードを携帯電話機に装着する。携帯電話機は、通常の電話機能の他にメモリカードからの暗号化コンテンツデータを復号し、かつ、再生して外部へ出力するための専用回路も有する。

【0013】このように、携帯電話機のユーザは、携帯電話機を用いて暗号化コンテンツデータを配信サーバから受信し、その暗号化コンテンツデータを再生することができる。

【0014】暗号化コンテンツデータの配信においては、たとえば、音楽データを試聴用の暗号化音楽データと配信用の暗号化音楽データとに分離し、まず、試聴用の音楽データを配信し、ユーザが試聴用の音楽データを復号および再生して試聴した結果、配信用の暗号化音楽データとライセンスの配信を希望するときに配信用の暗号化音楽データとライセンスを配信することが行なわれている。このような場合、試聴用音楽データは本体用音楽データに比べて音質が劣っていて、仮に、試聴用音楽データをダウンロードしても著作権者の権利を損なわないようになっている。

【0015】

【発明が解決しようとする課題】しかし、ユーザにとっては、試聴用音楽データによって購入しようとする音楽データの特長は可能であるが、提供される配信音楽データの音質について確認できない。また、試聴用音楽データと配信音楽データが同一である保証がない。

【0016】このような、問題は音楽データに限らず、朗読データ、教材データ、ビデオデータ、ゲーム等のコンテンツデータの配信において同様に生じる。

【0017】さらには、朗読データ、教材データ、ゲームなどのコンテンツデータにおいては、すべてのデータを一括で購入するのではなく、例えば、朗読データでは章ごとに、教材データやゲームなどではステージごとにユーザの配信要求に応じて配信する場合、複数回に分けて行なう配信に起因して、コンテンツデータの一括管理が難しくなるという問題が発生する。

【0018】そこで、本発明は、かかる問題を解決するためになされたものであり、その目的は、複数の領域に分離された暗号化コンテンツデータと、複数の領域に含まれる暗号化データを復号および再生するための複数のライセンスとを配信するコンテンツ提供方法を提供することである。

【0019】また、本発明の別の目的は、複数の領域に分離された暗号化コンテンツデータを複数のライセンスによって再生可能なデータ再生装置を提供することである。

【0020】さらに、本発明の別の目的は、複数の領域に分離された暗号化コンテンツデータと複数のライセンスとを記録したデータ記録装置を提供することである。

【0021】

【課題を解決するための手段】この発明によれば、コンテンツ提供方法は、コンテンツデータを暗号化した暗号化コンテンツデータの取得要求を受信する第1のステップと、第1のステップにおいて受信した取得要求に応じて、暗号化コンテンツデータを提供する第2のステップと、暗号化コンテンツデータの一部に対応し、かつ、一部を復号するための第1のライセンスの提供要求を受信する第3のステップと、第3のステップにおいて受信した提供要求に応じて、第1のライセンスを提供する第4のステップと、第1のライセンスと異なり、かつ、暗号化コンテンツデータの第1のライセンスに対応しない他の一部に対応し、他の一部を復号するための第2のライセンスの提供要求を受信する第5のステップと、第5のステップにおいて受信した提供要求に応じて、第2のライセンスを提供する第6のステップと、第2のライセンスの提供に対して課金処理を行なう第7のステップとを含む。

【0022】好ましくは、暗号化コンテンツデータ、第1のライセンス、および第2のライセンスが同じサーバから配信される。

【0023】好ましくは、暗号化コンテンツデータ、および第1のライセンスが第1のサーバから配信され、第2のライセンスが第1のサーバと異なる第2のサーバから配信される。

【0024】好ましくは、暗号化コンテンツデータ、および第1のライセンスは、記録媒体を介して第1のサーバに供給される。

【0025】好ましくは、暗号化コンテンツデータが第1のサーバから提供され、第1および第2のライセンスが第1のサーバと異なる第2のサーバから配信される。

【0026】好ましくは、暗号化コンテンツデータは、記録媒体を介して第1のサーバに供給される。

【0027】好ましくは、第3のステップにおいて、提供要求とともに認証データを受信し、認証データが認証されると第1のライセンスを提供し、第5のステップにおいて、提供要求とともに認証データを受信し、認証データが認証されると第2のライセンスを提供する。

【0028】また、この発明によれば、データ再生装置は、複数のブロックから成る暗号化コンテンツデータを複数のブロックに対応する複数のライセンスによって復号して再生するデータ再生装置であって、暗号化コンテンツデータ、および複数のライセンスが記録されたデータ記録装置とのやり取りを行なうインタフェースと、指示を入力するための操作部と、暗号化コンテンツデータを複数のライセンスによって復号して再生するコンテンツ再生部と、制御部とを備え、制御部は、コンテンツ再

生部において、暗号化コンテンツデータを構成する n 番目（ n は自然数）のブロックに含まれる暗号化データが n 番目のブロックに対応する n 番目のライセンスによって復号および再生されているときに、 $n+1$ 番目のライセンスをインタフェースを介してデータ記録装置から取得してコンテンツ再生部に与える。

【0029】好ましくは、コンテンツ再生部は、 n 番目のライセンスに含まれる n 番目のライセンス鍵を保持する第1のライセンス鍵保持部と、 $n+1$ 番目のライセンスに含まれる $n+1$ 番目のライセンス鍵を保持する第2のライセンス鍵保持部と、第1および第2のライセンス鍵保持部から n 番目のライセンス鍵と $n+1$ 番目のライセンス鍵とを選択的に取得し、その取得したライセンス鍵によって対応する暗号化データを復号する復号部と、復号部によって復号されたコンテンツデータを再生する再生部とを含む。

【0030】好ましくは、制御部は、鍵変更情報をインタフェースを介してデータ記録装置から取得し、鍵変更情報に基づいて n 番目のライセンス鍵と $n+1$ 番目のライセンス鍵とを選択して復号部に与える。

【0031】好ましくは、データ記録装置から複数のライセンスの各々を取得するセッションにおいて、異なるセッションキーを発生するセッションキー発生部と、セッションキー発生部によって発生されたセッションキーを受け、そのセッションキーによって暗号化ライセンス鍵を復号し、その復号したライセンス鍵を第1または第2のライセンス鍵保持部に与えるライセンス鍵復号部とをさらに備え、制御部は、セッションキー発生部によって発生されたセッションキーをインタフェースを介してデータ記録装置に入力し、セッションキーによって暗号化された暗号化ライセンス鍵をインタフェースを介してデータ記録装置から取得してライセンス鍵復号部に与える。

【0032】好ましくは、データ再生装置は、ライセンス鍵を提供するライセンス配信サーバからライセンス鍵をダウンロードするための通信を行なうデータ送受信部をさらに備え、制御部は、暗号化コンテンツデータの全部を再生するために必要なライセンスがデータ記録装置に記録されていないとき、データ記録装置に格納されている暗号化コンテンツデータに対応する複数のライセンスによって再生可能なブロックのみを暗号化コンテンツデータの再生順に従って、データ記録装置から取得してコンテンツ再生部に与え、操作部から入力される新たなライセンス鍵の取得指示に従ってライセンス配信サーバから暗号化コンテンツデータを構成するブロックに対応するライセンス鍵をデータ送受信部を介して受信し、その受信したライセンス鍵をデータ記録装置に記録する。

【0033】また、この発明によれば、データ記録装置は、複数のブロックから成る暗号化コンテンツデータおよび複数のブロックに含まれる複数の暗号化データを復

号するための複数のライセンスとを記録するデータ記録装置であって、複数のライセンスを格納するライセンス領域と、暗号化コンテンツデータと、複数のライセンスの各々と暗号化コンテンツデータを構成する複数のブロックとの対応を示すライセンス対応情報とを格納するデータ領域とを備える。

【0034】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【0035】図1は、本発明によるデータ記録装置が暗号化コンテンツデータを取得するデータ配信システムの全体構成を概念的に説明するための概略図である。

【0036】なお、以下では携帯電話網を介してデジタル音楽データをユーザの携帯電話機に装着されたメモリカード110に、またはインターネットを介してデジタル音楽データをカードライタに装着されたメモリカード110に配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば画像データ、動画データ等を配信する場合においても適用することが可能なものである。

【0037】図1を参照して、配信キャリア20は、自己の携帯電話網を通じて得た、ユーザからの配信要求（配信リクエスト）を配信サーバ10に中継する。著作権の存在する音楽データを管理する配信サーバ10は、データ配信を求めてアクセスして来た携帯電話ユーザの携帯電話機100に装着されたメモリカード110が正当な認証データを持つか否か、すなわち、コンテンツ保護機能を備えた正規のメモリカードであるか否かの認証処理を行ない、正規のメモリカードに対して暗号化コンテンツデータを復号するためのライセンスを配信する配信キャリア20である携帯電話会社に、このような暗号化コンテンツデータおよびライセンスを与える。

【0038】配信キャリア20は、自己の携帯電話網を通じて配信要求を送信した携帯電話機100に装着されたメモリカード110に対して、携帯電話網および携帯電話機100を介して暗号化コンテンツデータとライセンスとを配信する。

【0039】図1においては、たとえば携帯電話ユーザの携帯電話機100には、着脱可能なメモリカード110が装着される構成となっている。メモリカード110は、携帯電話機100により受信された暗号化コンテンツデータを受取り、上記配信にあたって行なわれた暗号化を復号した上で、携帯電話機100中の音楽再生部（図示せず）に与える。

【0040】さらに、たとえば携帯電話ユーザは、携帯電話機100に接続したヘッドホーン130等を介してこのようなコンテンツデータを「再生」して、聴取する

ことが可能である。

【0041】このような構成とすることで、まず、メモリカード110を利用しないと、配信サーバ10からコンテンツデータの配信を受けて、音楽を再生することが困難な構成となる。

【0042】しかも、配信キャリア20において、たとえば1曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、携帯電話ユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア20が携帯電話機の通話料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【0043】図1に示すデータ配信システムにおいては、暗号化コンテンツデータ {Dc} Kcは、ライセンス鍵Kc1にて復号可能な暗号化を施された領域である試験領域 {Dc1} Kc1と、ライセンス鍵Kc2にて暗号化を施された本体領域 {Dc2} Kc2とから成り、一つの暗号化コンテンツデータとして構成されている。したがって、試験には、ライセンス鍵Kc1を含む試験用ライセンスが必要であり、コンテンツ全体の再生には、試験用ライセンスとライセンス鍵Kc2を含む本体用ライセンスとが必要である。

【0044】配信サーバ10は、まず、携帯電話網を介して、暗号化コンテンツデータ {Dc} Kcと、ライセンス鍵Kc1を含む試験用ライセンスを携帯電話機100へ配信する。そして、ユーザは、携帯電話機100に備えられたコンテンツ再生回路（図示せず）において、暗号化コンテンツデータ {Dc} Kcの一部である試験領域 {Dc1} Kc1が試験用ライセンスのライセンス鍵Kc1によって復号され、再生された音楽を聴き、このコンテンツをダウンロードしたいと思うと、再度、配信サーバ10に対して本体用ライセンスの配信要求を送信する。そして、配信サーバ10は、受信した配信要求に応じてライセンス鍵Kc2を含む本体用ライセンスを携帯電話網を介して携帯電話機100に配信する。

【0045】そうすると、携帯電話機100のコンテンツ再生回路は、試験用ライセンスに含まれるライセンス鍵Kc1と本体用ライセンスに含まれるライセンス鍵Kc2を用いて暗号化コンテンツデータ {Dc} Kcの全てを再生できるようになる。

【0046】また、図1においては、配信サーバ10は、暗号化コンテンツデータ {Dc} Kc、およびライセンス鍵Kc1を含む試験用ライセンスをインターネット網30を介してパーソナルコンピュータ50に配信する。そして、パーソナルコンピュータ50は、USB（Universal Serial Bus）ケーブル70およびカードライター80を介して暗号化音楽データ {Dc} Kcおよびライセンス鍵Kc1を含む試験用ライセンスの配信要求を受け、カードライター80に装着されたメモリカード110の正当性を上述したのと同じ

方法によって判断し、正規なメモリカードに暗号化音楽データ {Dc} Kcおよびライセンス鍵Kc1を含む試験用ライセンスを記録する。そして、メモリカード110は、カードライター80から抜かれ、携帯電話機100に装着される。携帯電話機100のユーザは、装着されたメモリカード110から暗号化音楽データ {Dc} Kcおよびライセンス鍵Kc1を読出し、暗号化音楽データ {Dc} Kcの一部であるライセンス鍵Kc1によって復号可能な領域 {Dc1} Kc1を復号および再生して試験する。そして、ユーザは、暗号化音楽データ {Dc} Kcの全てを再生するためにライセンス鍵Kc2を含む本体用ライセンスのダウンロードを希望するとき、携帯電話網30を介して配信サーバ10へライセンス鍵Kc2を含む本体用ライセンスの配信要求を送信する。そうすると、配信サーバ10は、再び、メモリカード110が正規のメモリカードであることを確認した上でライセンス鍵Kc2を含む本体用ライセンスを携帯電話網を介して携帯電話機100へ配信する。そして、携帯電話機100は、受信したライセンス鍵Kc2を含む本体用ライセンスをメモリカード110に記録する。ユーザは、携帯電話機100を用いてメモリカード110に記録された暗号化音楽データ {Dc} Kcの全体はライセンス鍵Kc1およびライセンス鍵Kc2を用いて復号して再生する。

【0047】CD-ROM60は、暗号化コンテンツデータ {Dc} Kcと、暗号化コンテンツデータ {Dc} Kcの試験領域 {Dc1} Kc1を復号するためのライセンス鍵Kc1を含む試験用ライセンスとが記録されている。パーソナルコンピュータ50は、CD-ROM60から暗号化コンテンツデータ {Dc} Kcと、試験用ライセンスとを讀出す。そして、パーソナルコンピュータ50は、カードライター80に装着されたメモリカード110の正当性をカードライター80およびUSBケーブル70を介して確認し、正規なメモリカードにライセンス鍵Kc1を含む試験用ライセンスを記録する。そして、メモリカード110は、カードライター80から抜かれ、携帯電話機100に装着される。携帯電話機100のユーザは、装着されたメモリカード110から暗号化音楽データ {Dc} Kcの一部である試験領域 {Dc1} Kc1およびライセンス鍵Kc1を讀出し、暗号化音楽データ {Dc} Kcの一部を復号および再生して試験する。そして、ユーザは、ライセンス鍵Kc2を含む本体用ライセンスのダウンロードを希望するとき、携帯電話網30を介して配信サーバ10へライセンス鍵Kc2を含む本体用ライセンスの配信要求を送信する。

【0048】そうすると、配信サーバ10は、メモリカード110が正規のメモリカードであることを確認した上でライセンス鍵Kc2を含む本体用ライセンスを携帯電話網を介して携帯電話機100へ配信する。そして、携帯電話機100は受信したライセンス鍵Kc2をメモ

リカード110に記録する。ユーザは、携帯電話機100を用いてメモリカード110に記録された暗号化音楽データ{Dc}Kc、ライセンス鍵Kc1およびライセンス鍵Kc2を讀出して暗号化コンテンツデータ{Dc}Kcの全てを再生する。

【0049】この時、CD-ROM60に記録されている試験用ライセンスは暗号化された上で記録され、メモリカード110にライセンスを記録するための専用プログラムによってのみアクセスできるようになっている必要がある。CD-ROM60上のライセンスをそのまま複製しても暗号化コンテンツデータ{Dc}Kcの再生に用いることができない。

【0050】また、CD-ROM60は、暗号化音楽データ{Dc}Kcのみが記録されている。パーソナルコンピュータ50は、CD-ROM60から暗号化音楽データ{Dc}Kcを讀出す。そして、パーソナルコンピュータ50は、カードライター80およびUSBケーブル70を介して暗号化音楽データ{Dc}Kcをメモリカード110に記録する。そして、メモリカード110は、カードライター80から抜かれ、携帯電話機100に装着される。携帯電話機100のユーザは、装着されたメモリカード110に記録された暗号化音楽データ{Dc}Kcに対する試験用ライセンスの配信を携帯電話機網および配信キャリア20を介して配信サーバ10へ要求する。

【0051】図1に示すデータ配信システムにおいては、暗号化コンテンツデータ{Dc}Kcは、ライセンス鍵Kc1にて復号可能な暗号化を施された領域である試験領域{Dc1}Kc1と、ライセンス鍵Kc2にて暗号化を施された本体領域{Dc2}Kc2とから成り、一つの暗号化コンテンツデータとして構成されている。したがって、試験には、ライセンス鍵Kc1を含む試験用ライセンスが必要であり、コンテンツ全体の再生には、試験用ライセンスと、ライセンス鍵Kc2を含む本体用ライセンスとが必要となる。

【0052】配信サーバ10は、まず、携帯電話網を介して、暗号化コンテンツデータ{Dc}Kcと、ライセンス鍵Kc1を含む試験用ライセンスを携帯電話機100へ配信する。そして、ユーザは、携帯電話機100に備えられたコンテンツ再生回路(図示せず)において、暗号化コンテンツデータ{Dc}Kcの一部である試験用領域{Dc1}Kc1が試験用ライセンスのライセンス鍵Kc1によって復号され、かつ、再生された音楽を聴き、このコンテンツをダウンロードしたいと思うと、再度、配信サーバ10に対して本体用ライセンスの配信要求を送信する。そして、配信サーバ10は、受信した配信要求に応じてライセンス鍵Kc2を含む本体用ライセンスを携帯電話網を介して携帯電話機100に配信する。

【0053】そうすると、携帯電話機100のコンテン

ツ再生回路は、試験用ライセンスに含まれるライセンス鍵Kc1と本体用ライセンスに含まれるKc2を用いて暗号化コンテンツデータ{Dc}Kcのすべてを再生できるようにする。

【0054】また、説明は省略するが、試験用ライセンスと同様に本体用ライセンスもパーソナルコンピュータ50がインターネット網30を介して取得してメモリカード110に記録させることもできる。インターネット網30を介してパーソナルコンピュータ50に試験用ライセンスまたは本体用ライセンスを配信する場合は、暗号通信を用いる。

【0055】このように、メモリカード110は、各種の方法によって暗号化音楽データ{Dc}Kc、ライセンス鍵Kc1を含む試験用ライセンスおよびライセンス鍵Kc2を含む本体用ライセンスを取得する。

【0056】図1に示したような構成においては、暗号化して配信されるコンテンツデータを携帯電話機のユーザ側で再生可能とするためにシステム上必要とされるのは、第1には、通信におけるライセンス鍵を配信するための方式であり、さらに第2には、配信したいコンテンツデータを暗号化する方式そのものであり、さらに、第3には、このように配信されたコンテンツデータの無断コピーを防止するためのコンテンツデータ保護を実現する構成である。

【0057】本発明の実施の形態においては、特に、配信、および再生の各セッションの発生時において、これらのコンテンツデータの移動先に対する認証およびチェック機能を充実させ、非認証もしくは復号鍵の破られた記録装置およびデータ再生端末(コンテンツを再生できるデータ再生端末を携帯電話機とも言う。以下同じ)に対するコンテンツデータの出力を防止することによってコンテンツデータの著作権保護を強化する構成を説明する。

【0058】なお、以下の説明においては、配信サーバ10から各携帯電話機を介してメモリカードへ、またはパーソナルコンピュータからカードライターを介してメモリカードへコンテンツデータ(暗号化コンテンツデータおよびライセンス)を伝送する処理を「配信」と称することとする。

【0059】図2は、図1に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図である。

【0060】まず、配信サーバ10より配信されるデータについて説明する。Dcは、音楽データ等のコンテンツデータである。コンテンツデータDcは、ライセンス鍵Kcで復号可能な暗号化が施される。コンテンツデータDcは、試験領域Dc1と本体領域Dc2とから成り、それぞれ、異なる暗号鍵によって暗号化されている。試験領域Dc1は、ライセンス鍵Kc1によって復号可能な暗号化が施された試験領域{Dc1}Kc1と

して、また、本体領域Dc2は、ライセンス鍵Kc2によって復号可能な暗号化が施された本体領域{Dc2}Kc2として1つの暗号化コンテンツデータ{Dc}Kcを構成する。コンテンツデータDcは、必ず、暗号化された暗号化コンテンツデータ{Dc}Kcとして携帯電話機100またはパーソナルコンピュータ50へ配信される。その結果、全体としては、コンテンツデータDcは、ライセンス鍵Kc(Kc1とKc2とから成る)によって復号可能な暗号化が施された暗号化コンテンツデータ{Dc}Kcとして配信サーバ10より携帯電話機100またはパーソナルコンピュータ50のユーザに配布される。

【0061】なお、以下においては、{Y}Xという表記は、データYを、復号鍵Xにより復号可能な暗号化を施したことを示すものとする。

【0062】図3を参照して、情報データベース304が保持する暗号化コンテンツデータ{Dc}Kcのフォーマットについて説明する。暗号化コンテンツデータ{Dc}Kcが暗号化音楽データであるとき、暗号化コンテンツデータ{Dc}Kcは図3の(a)に示すフォーマットから成る。暗号化音楽データ90は、試験領域91({Dc1}Kc1)と本体領域92({Dc2}Kc2)とから成る。試験領域91({Dc1}Kc1)は、ライセンス鍵Kc1によって復号可能である。本体領域92({Dc2}Kc2)は、ライセンス鍵Kc2によって復号可能である。試験領域91({Dc1}Kc1)は、暗号化コンテンツデータ{Dc}Kcの途中に含まれ、本体領域92({Dc2}Kc2)が2分割されている。この場合、試験用の暗号化音楽データ91は、曲のサビから成る。試験領域91({Dc1}Kc1)は、1つの連続する領域として示したが、本体領域92({Dc2}Kc2)と同様に、本体領域92({Dc2}Kc2)によって分割された領域であってもよい。

【0063】また、暗号化コンテンツデータ{Dc}Kcは、図3の(b)に示すフォーマットから成っていてもよい。暗号化音楽データ93は、試験用の暗号化音楽データ94と本体用の暗号化音楽データ95とから成る。試験用の暗号化音楽データ94は、ライセンス鍵Kc1によって復号可能である。本体用の暗号化音楽データ95は、ライセンス鍵Kc2によって復号可能である。試験用の暗号化音楽データ94は、暗号化コンテンツデータ{Dc}Kcの最初に含まれている。この場合、試験用の暗号化音楽データ94は、曲のイントロから成る。

【0064】図4を参照して、暗号化コンテンツデータ{Dc}Kc84の生成について説明する。平文のコンテンツデータである源データDc81を最小暗号化単位であるMバイトの固定長を有するブロックBLK1, BLK2, ..., BLKkに分割してブロックデータ8

2を生成する(kは自然数)。最終ブロックBLKkがMバイトに満たないときは、意味を持たないダミーデータをデータ末尾に追加してMバイトのブロックを構成する(斜線部)。そして、ブロックBLK1, BLK2, ..., BLKkの各々を個々に暗号化して暗号化データ83を生成する。このとき、ブロックごとにライセンス鍵Kc1, Kc2のいずれに対応させるかが決定される。ライセンス鍵とブロックとの対応は付加情報Dc-inf内にライセンス鍵対応情報として記録される。その後、ブロックBLK1, BLK2, ..., BLKkの各々にヘッダを追加して暗号化コンテンツデータ{Dc}Kc84を生成する。すなわち、ブロックBLK1は、ヘッダ841と、暗号化データ842とから成り、ブロックBLK2は、ヘッダ843と暗号化データ844とから成り、ブロックBLKkは、ヘッダ845と暗号化データ846とから成る。ヘッダ841, 843, 845は、Nバイトのデータであり、そのブロックが暗号化ブロックであるか非暗号化ブロックであるかを示すスクランブルフラグが記録されている。つまり、ヘッダ841, 843, 845は、暗号化ブロックであることを示す「1」または非暗号化ブロックであることを示す「0」を含む。したがって、図3の示す暗号化コンテンツデータは、図4に示すデータフォーマットから成り、試験領域および本体領域は重複しない複数のブロックによって構成される。

【0065】再び、図2を参照して、配信サーバ10からは、暗号化コンテンツデータとともに、暗号化コンテンツデータに対するライセンス鍵対応情報、コンテンツデータの著作権に関する情報あるいはサーバアクセス関連情報等の平文情報としての付加情報Dc-infが配布される。また、ライセンスとして、ライセンス鍵Kc、配信サーバ10からのライセンス鍵等を特定するための管理コードであるライセンスIDが配信サーバ10と、携帯電話機100またはパーソナルコンピュータ50との間でやり取りされ、かつ、メモリカード110にライセンス鍵Kciとともに記録される。さらに、ライセンスとしては、コンテンツデータDcを識別するためのコードであるコンテンツIDや、利用者側からの指定によって決定されるライセンスの種類や機能限定等の情報を含んだライセンス購入条件ACに基づいて生成される、記録装置(メモリカード)におけるライセンスのアクセスに対する制限に関する情報であるアクセス制御情報ACmおよびデータ再生端末における再生に関する制御情報である再生制御情報ACp等が存在する。具体的には、アクセス制御情報ACmはメモリカードからのライセンスまたはライセンス鍵を外部に出力するに当たっての制御情報であり、再生可能回数(再生のためにライセンス鍵を出力する数)、およびライセンスの移動・複製に関する制限情報などがある。再生制御情報ACpは、再生するためにコンテンツ再生回路がライセンス鍵を受

取った後に、再生を制限する情報であり、再生期限、再生速度変更制限、再生範囲指定（部分ライセンス）などがある。

【0066】以後、コンテンツIDとライセンス鍵 K_{ci} （ $i=1, 2$ ）とライセンスIDとアクセス制御情報 AC_m と再生制御情報 AC_p とを併せて、ライセンスと総称することとする。ライセンス鍵 K_{c1} を含むライセンスが試験用ライセンスであり、ライセンス鍵 K_{c2} を含むライセンスが本体用ライセンスである。

【0067】また、以降では、簡単化のためアクセス制御情報 AC_m は再生回数の制限を行なう制御情報である再生回数（0：再生不可、1～254：再生可能回数、255：制限無し）、ライセンスの移動および複製を制限する移動・複製フラグ（1：移動複製不可、2：移動のみ可、3：移動複製禁止）の2項目とし、再生制御情報 AC_p は再生可能な期限を規定する制御情報である再生期限（UTCtimeコード）のみを制限するものとする。

【0068】図5は、図1に示すデータ配信システムにおいて使用される認証のためのデータ、情報等の特性を説明する図である。

【0069】コンテンツ再生回路、およびメモ리카ードには固有の公開暗号鍵 K_{py} および K_{pmw} がそれぞれ設けられ、公開暗号鍵 K_{py} および K_{pmw} はコンテンツ再生回路に固有の秘密復号鍵 K_{py} およびメモ리카ードに固有の秘密復号鍵 K_{mw} によってそれぞれ復号可能である。これら公開暗号鍵および秘密復号鍵は、コンテンツ再生回路、およびメモ리카ードの種類ごとに異なる値を持つ。これらの公開暗号鍵および秘密復号鍵を総称してクラス鍵と称し、これらの公開暗号鍵をクラス公開暗号鍵、秘密復号鍵をクラス秘密復号鍵、クラス鍵を共有する単位をクラスと称する。クラスは、製造会社や製品の種類、製造時のロット等によって異なる。

【0070】また、コンテンツ再生回路（携帯電話機、再生端末）のクラス証明書として C_{py} が設けられ、メモ리카ードのクラス証明書として C_{mw} が設けられる。これらのクラス証明書は、コンテンツ再生回路、およびメモ리카ードのクラスごとに異なる情報を有する。耐タンパモジュールが破られたり、クラス鍵による暗号が破られた、すなわち、秘密復号鍵が漏洩したクラスに対しては、禁止クラスリストにリストアップされてライセンス取得の禁止対象となる。

【0071】これらのコンテンツ再生回路のクラス公開暗号鍵およびクラス証明書は、認証データ $\{K_{py}/C_{py}\}$ K_{Pa} の形式で、メモ리카ードのクラス公開暗号鍵およびクラス証明書は認証データ $\{K_{pmw}/C_{mw}\}$ K_{Pa} の形式で、出荷時にデータ再生回路、およびメモ리카ードにそれぞれ記録される。後ほど詳細に説明するが、 K_{Pa} は配信システム全体で共通の公開認証鍵である。

【0072】また、メモ리카ード110内のデータ処理を管理するための鍵として、メモ리카ードという媒体ごとに設定される公開暗号鍵 K_{pmc} と、公開暗号鍵 K_{pmc} で暗号化されたデータを復号することが可能なそれぞれに固有の秘密復号鍵 K_{mc} が存在する。このメモ리카ードごとに個別な公開暗号鍵および秘密復号鍵を総称して個別鍵と称し、公開暗号鍵 K_{pmc} を個別公開暗号鍵、秘密復号鍵 K_{mc} を個別秘密復号鍵と称する。

【0073】メモ리카ード外とメモ리카ード間でのデータ授受でのデータ授受における秘密保持のための暗号鍵として、コンテンツデータの配信、および再生が行なわれるごとに配信サーバ10、携帯電話機100、およびメモ리카ード110において生成される共通鍵 $K_{s1} \sim K_{s3}$ が用いられる。

【0074】ここで、共通鍵 $K_{s1} \sim K_{s3}$ は、配信サーバ、コンテンツ再生回路もしくはメモ리카ード間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵 $K_{s1} \sim K_{s3}$ を「セッションキー」とも呼ぶこととする。

【0075】これらのセッションキー $K_{s1} \sim K_{s3}$ は、各セッションごとに固有の値を有することにより、配信サーバ、コンテンツ再生回路、およびメモ리카ードによって管理される。具体的には、セッションキー K_{s1} は、配信サーバによって配信セッションごとに発生される。セッションキー K_{s2} は、メモ리카ードによって配信セッションおよび再生セッションごとに発生し、セッションキー K_{s3} は、コンテンツ再生回路において再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行した上でライセンス鍵等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

【0076】なお、カードライタ80とUSBケーブル70を介してパーソナルコンピュータ50とメモ리카ード110との間の通信においては、配信サーバ10と携帯電話機100の機能をパーソナルコンピュータ50に読替え、メモ리카ードインタフェース1200をカードライタ80およびUSBケーブル70に読替えればよい。

【0077】図6は、図1に示した配信サーバ10の構成を示す概略ブロック図である。配信サーバ10は、コンテンツデータを所定の方式に従って暗号化したデータやコンテンツID等の配信情報を保持するための情報データベース304と、携帯電話機の各ユーザごとにコンテンツデータへのアクセス開始に従った課金情報を保持するための課金データベース302と、情報データベース304に保持されたコンテンツデータのメニューを保

持するメニューデータベース307と、ライセンスの配信ごとにコンテンツデータおよびライセンス鍵等の配信を特定するトランザクションID等の配信に関するログを保持する配信記録データベース308と、情報データベース304、課金データベース302、メニューデータベース307、および配信記録データベース308からのデータをバスBS1を介して受取り、所定の処理を行なうためのデータ処理部310と、通信網を介して、配信キャリア20とデータ処理部310との間でデータ授受を行なうための通信装置350とを備える。

【0078】暗号化コンテンツデータ{Dc}Kcが朗読データ、教材データ、またはゲームソフトのデータであるとき、暗号化コンテンツデータ{Dc}Kcは、図13の(c)に示すフォーマットから成る。暗号化コンテンツデータ96は、複数の領域961~967から成る。各領域961~967は、それぞれ、ライセンス鍵Kc1、Kc2、Kc3、Kc4、Kc5、Kc6、Kc7によって復号可能である。

【0079】暗号化コンテンツデータ{Dc}Kcが既に説明した音楽データと同様に試しようの領域を備えたビデオデータであるとき、暗号化コンテンツデータ{Dc}Kcは、図13の(d)に示すフォーマットから成る。暗号化データ97は、付属用の領域971と本体用の領域972とから成る。付属用の領域971は、ライセンス鍵Kc1によって復号可能である。本体用の領域972は、ライセンス鍵Kc2によって復号可能である。付属用の領域971は、ビデオまたはゲームのサブタイトルから成る。暗号化コンテンツデータ96、97の復号については、図7に示すコンテンツ再生回路1550が受理可能である。この場合、音楽再生部1520が各コンテンツに適合した再生回路に置換えられる。

【0080】データ処理部310は、バスBS1上のデータに応じて、データ処理部310の動作を制御するための配信制御部315と、配信制御部315に制御されて、配信セッション時にセッションキーKs1を発生するためのセッションキー発生部316と、メモリカードから送られてきた認証のための認証データ{Kpmw/Cmw}KPaを復号するための2種類の公開認証鍵KPaを保持する認証鍵保持部313と、メモリカードから送られてきた認証のための認証データ{Kpmw/Cmw}KPaを通信装置350およびバスBS1を介して受けて、認証鍵保持部313からの公開認証鍵KPaによって復号処理を行なう復号処理部312と、配信セッションごとに、セッション鍵Ks1を発生するセッションキー発生部316、セッションキー発生部316より生成されたセッションキーKs1を復号処理部312によって得られたクラス公開暗号鍵Kpmwを用いて暗号化して、バスBS1に出力するための暗号化処理部318と、セッションキーKs1によって暗号化された上で送信されたデータをバスBS1より受けて、復号

処理を行なう復号処理部320とを含む。

【0081】データ処理部310は、さらに、配信制御部315から与えられるライセンス鍵Kcおよびアクセス制御情報ACmを、復号処理部320によって得られたメモリカードごとに個別公開暗号鍵Kpmcによって暗号化するための暗号化処理部326と、暗号化処理部326の出力を、復号処理部320から与えられるセッションキーKs2によってさらに暗号化してバスBS1に出力するための暗号化処理部328とを含む。

【0082】配信サーバ10の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【0083】図7は、図1に示した携帯電話機100の構成を説明するための概略ブロック図である。

【0084】携帯電話機100は、携帯電話機100の各部のデータ授受を行なうためのバスBS2と、携帯電話網により無線伝送される信号を受信するためのアンテナ1101と、アンテナからの信号を受けてベースバンド信号に変換し、あるいは携帯電話機からのデータを変調してアンテナ1101に与えるための送受信部1102とを含む。

【0085】携帯電話機100は、さらに、携帯電話機100のユーザの音声データを取込むためのマイク1103と、マイク1103からの音声データをアナログ信号からデジタル信号に変換するAD変換器1104と、AD変換器1104からの音声データを所定の方式に変調する音声符号化部1105とを含む。

【0086】携帯電話機100は、さらに、アンテナ1101および送受信部1102を介して受信した他の携帯電話機のユーザの音声データを再生する音声再生部1106と、音声再生部1106からのデータをデジタル信号からアナログ信号へ変換するDA変換器1107と、DA変換器1107からの音声データを外部へ出力するスピーカ1108とを含む。

【0087】携帯電話機100は、さらに、バスBS2を介して携帯電話機100の動作を制御するためのコントローラ1109と、外部からの指示を携帯電話機100に与えるための操作パネル1111と、コントローラ1109等から出力される情報をユーザに視覚情報として与えるための表示パネル1110とを含む。

【0088】携帯電話機100は、さらに、配信サーバ10からのコンテンツデータ(音楽データ)を記憶し、かつ、復号処理を行なうための着脱可能なメモリカード1110と、メモリカード1110とバスBS2との間のデータの授受を制御するためのメモリカードインタフェース1200とを含む。

【0089】携帯電話機100は、さらに、クラス公開暗号鍵Kpp1およびクラス証明書Cp1を公開認証鍵KPaで復号することでその正当性を認証できる状態に暗号化した認証データ{Kpp1/Cp1}KPaを

保持する認証データ保持部1500を含む。ここで、再生端末102のクラス y は、 $y=1$ であるとする。

【0090】携帯電話機100は、さらに、クラス固有の復号鍵である $Kp1$ を保持する $Kp1$ 保持部1502と、バスBS2から受けたデータを $Kp1$ によって復号し、メモリカード110によって発生されたセッションキー $Ks2$ を得る復号処理部1504とを含む。

【0091】携帯電話機100は、さらに、メモリカード110に記憶されたコンテンツデータの再生を行なう再生セッションにおいてメモリカード110との間でバスBS2上においてやり取りされるデータを暗号化するためのセッションキー $Ks3$ を乱数等により発生するセッションキー発生部1508と、暗号化コンテンツデータの再生セッションにおいてメモリカード110からライセンス鍵 Kc ($Kc1$ と $Kc2$ とから成る。以下同じ) および再生制御情報 AcP を受取る際に、セッションキー発生部1508により発生されたセッションキー $Ks3$ を復号処理部1504によって得られたセッションキー $Ks2$ によって暗号化し、バスBS2に出力する暗号化処理部1506とを含む。

【0092】携帯電話機100は、さらに、バスBS2上のデータをセッションキー $Ks3$ によって復号して、ライセンス鍵 Kc および再生制御情報 AcP を出力する復号処理部1510と、コントローラ1109からの指示によって復号処理部1510から出力されたライセンス鍵 $Kc1$ 、 $Kc2$ のいずれか一方を端子1512を介して Kc 保持部1514へ出力し、端子1513を介してライセンス鍵 $Kc1$ 、 $Kc2$ のいずれか他方を Kc 保持部1515へ出力するスイッチ1511とを含む。

【0093】携帯電話機100は、さらに、端子1512から入力されたライセンス鍵 $Kc1$ 、 $Kc2$ のいずれかを保持する Kc 保持部1514と、端子1513から入力された Kc 保持部1514が保持するライセンス鍵とは異なるライセンス鍵、すなわち、 Kc 保持部1514がライセンス鍵 $Kc1$ を保持するときライセンス鍵 $Kc2$ を保持する Kc 保持部1515とを含む。

【0094】携帯電話機100は、さらに、 Kc 保持部1514または Kc 保持部1515に保持される2つのライセンス鍵 $Kc1$ 、 $Kc2$ のいずれか1つを選択して復号処理部1519へ出力するスイッチ1518を含む。スイッチ1518は、 Kc 保持部1514からのライセンス鍵を受ける端子1516と、 Kc 保持部1515からのライセンス鍵を受ける端子1517とを含む。なお、スイッチ1518は、コントローラ1109からの指示によって端子1516または端子1517を選択してライセンス鍵 $Kc1$ またはライセンス鍵 $Kc2$ を復号処理部1519へ出力する。

【0095】携帯電話機100は、さらに、バスBS2より暗号化コンテンツデータ $\{Dc\} Kc$ を受けて、スイッチ1518から入力されたライセンス鍵 $Kc1$ また

は $Kc2$ によって暗号化コンテンツデータ $\{Dc\} Kc$ を復号する復号処理部1519とを含む。試験用ライセンスのみをメモリカード110に記録している場合には、ライセンス鍵 $Kc1$ にて復号再生可能な試験領域

$\{Dc1\} Kc1$ のみ再生可能である。

【0096】携帯電話機100は、さらに、復号処理部1519からの出力を受けてコンテンツデータを再生するための音楽再生部1520と、音楽再生部1520の出力をデジタル信号からアナログ信号に変換するDA変換器1521と、DA変換器1521の出力をヘッドホンなどの外部出力装置(図示省略)へ出力するための端子1522とを含む。

【0097】なお、図7においては、点線で囲んだ領域は暗号化コンテンツデータを復号して音楽データを再生するコンテンツ再生回路1550を構成する。

【0098】携帯電話機100の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【0099】図8は、図1に示すメモリカード110の構成を説明するための概略ブロック図である。

【0100】既に説明したように、メモリカードのクラス公開暗号鍵およびクラス秘密復号鍵として、 $KPmw$ および Kmw が設けられ、メモリカードのクラス証明書 Cmw が設けられるが、メモリカード110においては、自然数 $w=3$ で表わされるものとする。また、メモリカードを識別する自然数 x は $x=4$ で表わされるものとする。

【0101】したがって、メモリカード110は、認証データ $\{KPm3//Cm3\} KP a$ を保持する認証データ保持部1400と、メモリカードごとに設定される固有の復号鍵である個別秘密復号鍵 $Kmc4$ を保持する Kmc 保持部1402と、クラス秘密復号鍵 $Km3$ を保持する Km 保持部1421と、個別秘密復号鍵 $Kmc4$ によって復号可能な公開暗号鍵 $KPmc4$ を保持する $KPmc$ 保持部1416とを含む。

【0102】このように、メモリカードという記録装置の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたライセンス鍵の管理をメモリカード単位で実行することが可能になる。

【0103】メモリカード110は、さらに、メモリカードインタフェース1200との間で信号を端子1426を介して授受するインタフェース1424と、インタフェース1424との間で信号をやり取りするバスBS4と、バスBS4にインタフェース1424から与えられるデータから、クラス秘密復号鍵 $Km3$ を Km 保持部1421から受けて、配信サーバ10が配信セッションにおいて生成したセッションキー $Ks1$ を接点Paに出力する復号処理部1422と、 KPa 保持部1414から公開認証鍵 KPa を受けて、バスBS4に与えられる

データから公開認証鍵KPaによる復号処理を実行して復号結果と得られたクラス証明書をコントローラ1420に、得られたクラス公開鍵を暗号化処理部1410に出力する復号処理部1408と、切換スイッチ1442によって選択的に与えられる鍵によって、切換スイッチ1446によって選択的に与えられるデータを暗号化してバスBS4に出力する暗号化処理部1406とを含む。

【0104】メモリカード110は、さらに、配信、および再生の各セッションにおいてセッションキーKs2を発生するセッションキー発生部1418と、セッションキー発生部1418の出力したセッションキーKs2を復号処理部1408によって得られるクラス公開暗号鍵KppyもしくはKpmwによって暗号化してバスBS4に送出する暗号化処理部1410と、バスBS4よりセッションキーKs2によって暗号化されたデータを受けてセッションキー発生部1418より得たセッションキーKs2によって復号する復号処理部1412と、暗号化コンテンツデータの再生セッションにおいてメモリ1415から読出されたライセンス鍵Kcおよび再生制御情報ACpを、復号処理部1412で復号された他のメモリカード110の個別公開暗号鍵Kpmcx (x≠4)で暗号化する暗号化処理部1417とを含む。

【0105】メモリカード110は、さらに、バスBS4上のデータを個別公開暗号鍵Kpmc4と対をなすメモリカード110の個別秘密復号鍵Kmc4によって復号するための復号処理部1404と、暗号化コンテンツデータ[Dc]Kcと、暗号化コンテンツデータ[Dc]Kcを再生するためのライセンス(Kc, ACp, ACm, ライセンスID, コンテンツID)と、付加情報DoinfとをバスBS4より受けて格納するためのメモリ1415とを含む。メモリ1415は、例えば半導体メモリによって構成される。また、メモリ1415は、ライセンス領域1415Aと、データ領域1415Bとから成る。ライセンス領域1415Aは、ライセンスを記録するための領域である。データ領域1415Bは、暗号化コンテンツデータ[Dc]Kc、および暗号化コンテンツデータの付加情報Doinfを記録するための領域である。なお、データ領域1415Bは、外部からアクセス可能である。

【0106】メモリカード110は、さらに、バスBS4を介して外部との間でデータ授受を行ない、バスBS4との間で再生情報等を受けて、メモリカード110の動作を制御するためのコントローラ1420を含む。

【0107】なお、ライセンス領域1415Aは、耐タンパモジュール領域に構成される。また、ライセンス領域1415Aとデータ領域1415Bとは、1つのメモリ1415内に構成されている必要はなく、それぞれ、別々に構成されていても良い。さらに、メモリ1415は、データ領域1415Bを伴わないライセンス専用の

領域であってもよい。

【0108】以下、図1に示すデータ配信システムにおける各セッションの動作について説明する。

【0109】〔試聴用配信〕図1に示す配信サーバ10は、携帯電話網を介して携帯電話機100に装着されたメモリカード110に暗号化音楽データ[Dc]Kc、ライセンス鍵Kc1を含む試聴用ライセンス、およびライセンス鍵Kc2を含む本体用ライセンスを配信する動作について説明する。図9は、配信サーバ10からメモリカード110への暗号化音楽データ[Dc]Kc、ライセンス鍵Kc1を含む試聴用ライセンス、およびライセンス鍵Kc2の配信の全体動作を示すフローチャートである。携帯電話機100は、携帯電話機100のユーザの指示に応じて、携帯電話網を介して配信サーバ10へ暗号化音楽データ[Dc]Kcおよびライセンス鍵Kc1を含む試聴用ライセンスの配信要求を送信し、配信サーバ10から暗号化音楽データ[Dc]Kcおよび試聴用ライセンスを受信する。そして、携帯電話機100は、受信した暗号化音楽データ[Dc]Kcおよびライセンス鍵Kc1を含む試聴用ライセンスをメモリカード110に記録する(ステップS10)。その後、携帯電話機100は、ユーザからの試聴指示に応じて、メモリカード110から暗号化音楽データ[Dc]Kcの一部である試聴領域[Dc1]Kc1およびライセンス鍵Kc1を読み出し、コンテンツ再生回路1550において試聴用のライセンスに含まれるライセンス鍵Kc1によって復号可能な暗号化音楽データ[Dc1]Kc1を復号および再生する。そして、ユーザは、再生された音楽データをヘッドホン130を介して試聴する(ステップS20)。

【0110】ユーザは、試聴した音楽データの購入を希望するとき、ライセンス鍵Kc2を含む本体用ライセンスのダウンロード要求を携帯電話機100に入力する。そうすると、携帯電話機100は、携帯電話網を介してライセンス鍵Kc2を含む本体用ライセンスの配信要求を配信サーバ10へ送信し、配信サーバ10からライセンス鍵Kc2を含む本体用ライセンスを受信し、その受信したライセンス鍵Kc2を含む本体用ライセンスをメモリカード110に記録する(ステップS30)。その後、携帯電話機100は、ユーザの再生要求に応じて、暗号化音楽データ[Dc]Kcおよび2つのライセンス鍵Kc1、Kc2をメモリカード110から読み出し、コンテンツ再生回路1550において暗号化音楽データ[Dc]Kcを、暗号化コンテンツデータ[Dc]Kcの各領域に適合したライセンス鍵Kc1およびライセンス鍵Kc2を用いて復号および再生する。

【0111】以下、ステップS10、S20、S30の詳細について説明する。図10および図11は、図9のステップS10およびステップS30におけるライセンスの配信処理の詳細な動作を説明するためのフローチャ

ートである。まず、試験用のライセンスおよび暗号化コンテンツデータ {Dc} Kcを配信サーバ10からダウンロードするステップS10の詳細について説明する。

【0112】図10における処理以前に、携帯電話機100のユーザは、配信サーバ10に対して電話網を介して接続し、購入を希望するコンテンツに対するコンテンツIDを取得し、必要とするライセンスの種類を決定していることを前提としている。また、フローチャートにおけるライセンス鍵Kci (i=1, 2) は、Kc1またはKc2のいずれかのライセンス鍵であり、この場合、ライセンス鍵Kc1を含む試験用ライセンスの取得を目的としているため、i=1である。図10および図11におけるライセンス鍵Kciのiをi=1と読替えて試験用ライセンスの配信を説明する。

【0113】図10を参照して、携帯電話機100のユーザから操作パネル1111を介してコンテンツIDの指定による配信リクエストがなされる(ステップS100)。そして、操作パネル1111を介して試験用の暗号化音楽データ {Dc1} Kc1のライセンスKc1を購入するための購入条件ACが入力される(ステップS102)。つまり、選択した暗号化音楽データ {Dc} Kcを復号するライセンス鍵Kciをダウンロードするための条件として、ライセンス鍵Kc1なのか、ライセンス鍵Kc2なのか、すなわち試験用ライセンスなのか本体用ライセンスなのかを指示する。さらに、本体用ライセンスの場合には、暗号化コンテンツデータのアクセス制御情報ACm、および再生制御情報ACpを設定するための条件がライセンス購入条件ACとして入力される。

【0114】暗号化コンテンツデータの購入条件ACが入力されると、コントローラ1109は、バスBS2およびメモリカードインタフェース1200を介してメモリカード110へ認証データの出力指示を与える(ステップS104)。メモリカード110のコントローラ1420は、端子1426、インタフェース1424およびバスBS4を介して認証データの送信要求を受信する(ステップS106)。そして、コントローラ1420は、バスBS4を介して認証データ保持部1400から認証データ {Kpm3//Cm3} KPaを読み出し、

{Kpm3//Cm3} KPaをバスBS4、インタフェース1424および端子1426を介して出力する(ステップS108)。

【0115】携帯電話機100のコントローラ1109は、メモリカード110からの認証データ {Kpm3//Cm3} KPaに加えて、コンテンツID、ライセンス購入条件のデータAC、および配信リクエストを配信サーバ10に対して送信する(ステップS110)。

【0116】配信サーバ10では、携帯電話機100から配信リクエスト、コンテンツID、認証データ {Kpm3//Cm3} KPa、およびライセンス購入条件の

データACを受信し(ステップS112)、復号処理部312においてメモリカード110から出力された認証データを公開認証鍵KPaで復号処理を実行する(ステップS114)。

【0117】配信制御部315は、復号処理部312における復号処理結果から、正規の機関でその正当性を証明するための暗号化を施した認証データを受信したか否かを判断する認証処理を行なう(ステップS116)。正当な認証データであると判断された場合、配信制御部315は、クラス公開暗号鍵Kpm3およびクラス証明書Cm3を承認し、受理する。そして、次の処理(ステップS118)へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵Kpm3およびクラス証明書Cm3を受理しないで配信セッションを終了する(ステップS164)。

【0118】認証の結果、正当な認証データを持つメモリカードを装着した携帯電話機からのアクセスであることが確認されると、配信サーバ10において、セッションキー発生部316は、配信のためのセッションキーKs1を生成する(ステップS118)。セッションキーKs1は、復号処理部312によって得られたメモリカード110に対応するクラス公開暗号鍵Kpm3によって、暗号化処理部318によって暗号化される(ステップS120)。

【0119】配信制御部315は、ライセンスIDを生成し(ステップS122)、ライセンスIDおよび暗号化されたセッションキーKs1は、ライセンスID//{Ks1} Km3として、バスBS1および通信装置350を介して外部に出力される(ステップS124)。

【0120】携帯電話機100が、ライセンスID//{Ks1} Km3を受信すると、コントローラ1109は、ライセンスID//{Ks1} Km3をメモリカード110に入力する(ステップS126)。そうすると、メモリカード110においては、端子1426およびインタフェース1424を介して、コントローラ1420は、ライセンスID//{Ks1} Km3を受信する(ステップS128)。そして、コントローラ1420は、バスBS4を介して{Ks1} Km3を復号処理部1422へ与え、復号処理部1422は、保持部1421に保持されるメモリカード110に固有なクラス秘密復号鍵Km3によって復号処理することにより、セッションキーKs1を復号し、セッションキーKs1を受理する(ステップS132)。

【0121】コントローラ1420は、配信サーバ10で生成されたセッションキーKs1の受理を確認すると、セッションキー発生部1418に対してメモリカード110において配信動作時に生成されるセッションキーKs2の生成を指示する。そして、セッションキー発生部1418は、セッションキーKs2を生成する(ステップS134)。

【0122】暗号化処理部1406は、切換スイッチ1442の接点Paを介して復号処理部1422より与えられるセッションキーKs1によって、切換スイッチ1446の接点を順次切換えることによって与えられるセッションキーKs2、および個別公開暗号鍵KPmc4を1つのデータ列として暗号化して、{Ks2//KPmc4} Ks1をバスBS4に出力する。バスBS4に出力された暗号化データ{Ks2//KPmc4} Ks1は、バスBS4からインタフェース1424および端子1426を介して携帯電話機100に出力され(ステップS138)、携帯電話機100から配信サーバ10に送信される(ステップS140)。

【0123】図11を参照して、配信サーバ10は、

{Ks2//KPmc4} Ks1を受信して、復号処理部320においてセッションキーKs1による復号処理を実行し、メモリカード110で生成されたセッションキーKs2、およびメモリカード110に固有の公開暗号鍵KPmc4を受理する(ステップS142)。

【0124】配信制御部315は、ステップS112で取得したコンテンツIDと購入条件ACに従ってライセンス鍵Kc1を情報データベース304から取得し(ステップS144)、ステップS112で取得したライセンス購入条件のデータACに従って、アクセス制御情報ACmおよび再生制御情報ACpを決定する(ステップS146)。

【0125】配信制御部315は、生成したライセンス、すなわち、ライセンスID、コンテンツID、ライセンス鍵Kc、再生制御情報ACp、およびアクセス制御情報ACmを暗号化処理部326に与える。暗号化処理部326は、復号処理部320によって得られたメモリカード110に固有の公開暗号鍵KPmc4によってライセンスを暗号化して暗号化データ{ライセンスID//コンテンツID//Kc1//ACm//ACp} Kmc4を生成する(ステップS148)。そして、暗号化処理部328は、暗号化処理部326からの暗号化データ{ライセンスID//コンテンツID//Kc1//ACm//ACp} Kmc4を、復号処理部320からのセッションキーKs2によって暗号化し、暗号化データ[{ライセンスID//コンテンツID//Kc1//ACm//ACp} Kmc4] Ks2を出力する。配信制御部315は、バスBS1および通信装置350を介して暗号化データ[{ライセンスID//コンテンツID//Kc1//ACm//ACp} Kmc4] Ks2を携帯電話機100へ送信する(ステップS150)。

【0126】携帯電話機100は、送信された暗号化データ[{ライセンスID//コンテンツID//Kc1//ACm//ACp} Kmc4] Ks2を受信し、バスBS2を介してメモリカード110に入力する(ステップS152)。メモリカード110においては、端子

1426およびインタフェース1424を介して、バスBS4に与えられた受信データを復号処理部1412によって復号する。復号処理部1412は、セッションキー発生部1418から与えられたセッションキーKs2を用いてバスBS4の受信データを復号し、バスBS4に出力する(ステップS154)。

【0127】この段階で、バスBS4には、Kmc保持部1402に保持される秘密復号鍵Kmc4で復号可能な暗号化ライセンス{ライセンスID//コンテンツID//Kc1//ACm//ACp} Kmc4が出力される(ステップS154)。

【0128】コントローラ1420の指示によって、暗号化ライセンス{ライセンスID//コンテンツID//Kc1//ACm//ACp} Kmc4は、復号処理部1404において、個別秘密復号鍵Kmc4によって復号され、ライセンス(ライセンス鍵Kc1、ライセンスID、コンテンツID、アクセス制御情報ACmおよび再生制御情報ACp)が受理される(ステップS156)。

【0129】そうすると、メモリカード110のコントローラ1420は、受理したライセンス(ライセンスID、コンテンツID、ライセンス鍵Kc1、アクセス制御情報ACm、および再生制御情報ACp)を、ライセンス領域1415Aに格納する(ステップS160)。そして、配信サーバ10において、課金処理が行なわれる。すなわち、配信制御部315は、課金情報を課金データベース302に記録する(ステップS162)。なお、この場合の試験用ライセンスの配信に対する課金料金は、後述する本体用ライセンスの配信に対する課金料金よりも低い。そして、ライセンスの配信動作は終了する(ステップS164)。

【0130】暗号化コンテンツデータ{Dc} Kcについては、単なるダウンロード処理であるため詳細には説明しないが、試験用ライセンスの配信動作が終了した後、携帯電話機100のコントローラ1109は、暗号化コンテンツデータの配信要求を配信サーバ10へ送信し、配信サーバ10は、暗号化コンテンツデータの配信要求を受信する。そして、配信サーバ10の配信制御部315は、情報データベース304より、暗号化コンテンツデータ{Dc} Kcおよび付加情報Dc-infを取得して、これらのデータをバスBS1および通信装置350を介して出力する。

【0131】携帯電話機100は、{Dc} Kc//Dc-infを受信して、暗号化コンテンツデータ{Dc} Kcおよび付加情報Dc-infを受理する。そうすると、コントローラ1106は、暗号化コンテンツデータ{Dc} Kcおよび付加情報Dc-infをバスBS2およびメモリカードインタフェース1200を介してメモリカード110に入力する。メモリカード110のコントローラ1420は、受理した暗号化コンテンツ

データ {Dc} Kcおよび付加情報Dc-infをメモリ1415のデータ領域1415Bに記録する。なお、付加情報Dc-infには、暗号化コンテンツデータ

{Dc} Kcのうち、どのブロックをどのライセンス鍵によって復号すべきかを示すライセンス鍵を変更するためのライセンスとブロックの対応情報とが含まれる。

【0132】このようにして、ライセンスの配信においては、携帯電話機100に装着されたメモリカード110が正規の認証データを保持する機器であること、同時に、クラス証明書Cm3とともに暗号化して送信できた公開暗号鍵Kpm3が有効であることを確認した上でコンテンツデータを配信することができ、不正なメモリカードへのコンテンツデータの配信を禁止することができる。

【0133】さらに、配信サーバおよびメモリカードでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向上させることができる。

【0134】なお、上記において、試聴用ライセンスの配信に対して課金するとして説明したが（ステップS162）、試聴は、本体用ライセンスをダウンロードしてもらうことを目的としたサービスであり、より多くのユーザに聴いてもらう必要があるため、試聴用ライセンスの配信に対しては課金をしないことも可能である。

【0135】〔試聴〕次に、ステップS20における試聴について詳細に説明する。試聴用の再生においては、携帯電話機100のコントローラ1109は、メモリカード110から再生を行なう楽曲の付加データDc-infを読み出して、試聴用ライセンスにて再生可能な試聴用領域{Dc1} Kc1を構成するブロックを特定し、特定されたブロックのみにて構成される1つの新しい暗号化コンテンツデータを仮想的に生成し、この仮想的に生成された暗号化コンテンツデータを復号して再生する。図3の(a)を参照して、暗号化コンテンツデータ{Dc} Kcが暗号化コンテンツデータ90である場合には、試聴領域91（{Dc1} Kc1）を構成するブロックを確認し、該当するブロックのみから構成されるデータ列を一つの楽曲として再生する。図3の(b)を参照して、暗号化コンテンツデータ{Dc} Kcが暗号化コンテンツデータ93である場合も同様に、試聴領域94（{Dc1} Kc1）を一つの楽曲として再生する。

【0136】再生は、まず、メモリカード110に格納されている試聴用ライセンスに含まれるライセンス鍵Kc1をコンテンツ再生回路1550内の2つのKc保持部1514、1515のいずれかに保持させる「再生許諾」と、「再生許諾」後に、Kc保持部1514、15

15のいずれかに保持されているライセンス鍵Kc1をスイッチ1518にて選択して復号処理部1519に供給する。試聴用に仮想的に構成された暗号化コンテンツデータは試聴用領域{Dc1} Kc1と対応する。したがって、試聴用に仮想的に構成された暗号化コンテンツデータを、暗号化コンテンツデータ{Dc1} Kc1とも表すものとする。

【0137】そうすると、コントローラ1109はメモリカード110から暗号化コンテンツデータ{Dc1} Kc1を構成するブロックを再生順序に従って読み出して復号処理部1519に供給する。復号処理部1519は、入力された暗号化コンテンツデータを構成するブロックをライセンス鍵Kc1によって、それぞれ復号し、暗号化コンテンツデータ{Dc1} Kc1を復号して得られるコンテンツデータを構成する平文化されたブロック（源データを構成するブロック）を抽出する。そして、復号処理部1519は、抽出したブロックを音楽再生部1520に出力する。音楽再生部1520は、復号処理部1519から供給されるブロックに含まれるデータに基づいて、音楽をデジタル再生し、AD変換器1521へ供給する。そうすると、AD変換器1521は、コンテンツデータをデジタル信号からアナログ信号に変換して端子1522へ出力する。そして、暗号化コンテンツデータ{Dc1} Kc1を構成する全てのブロックが再生順に、メモリカード110から読み出され、一連の処理が終了すると試聴用の再生が終了する。ユーザは、端子1522に接続されたヘッドホン130等によってこの暗号化コンテンツデータ{Dc} Kcの試聴領域{Dc1} Kc1を試聴することができる。

【0138】このとき、再生の対象となる全てのブロックに対する一連の処理が終了すると試聴用の再生が終了すると説明したが、繰り返し試聴することを前提として、再生の対象となる全てのブロックの読み出しが終了すると、暗号化コンテンツデータ{Dc1} Kc1の先頭のブロックにもどって連続して再生するように構成することも可能である。この場合、試聴の終了は、ユーザが操作パネル1111を操作して、試聴の終了をコントローラ1109に指示し、コントローラ1109が、指示に従って再生を終了するように構成する。

【0139】次に、試聴用ライセンスに含まれるライセンス鍵Kc1をコンテンツ再生回路1550内の2つのKc保持部1514、1515のいずれかに保持させる「再生許諾」について説明する。図12は「再生許諾」の動作を説明するためのフローチャートである。「再生許諾」は試聴用ライセンスのライセンス鍵Kc1をKc保持部1514、1515のいずれかに保持させるのみでなく、本体用ライセンスのライセンス鍵Kc2をKc保持部1514、1515のいずれかに保持させる処理でもあり、図12ではライセンス鍵はKciと表記されている。試聴においてはライセンス鍵を区別する識別子

i が i = 1 と読替えて説明を行なう。また、ライセンス鍵 Kc1 は Kc 保持部 1514 に保持されるものとして説明を行なう。

【0140】図12を参照して、試聴のための再生動作が開始されると、携帯電話機100のユーザから操作パネル1111を介して再生許諾リクエストが携帯電話機100にインプットされる(ステップS200)。そうすると、コントローラ1109は、バスBS2を介して認証データの出力要求をコンテンツ再生回路1550に行ない(ステップS202)、コンテンツ再生回路1550は認証データの出力要求を受信する(ステップS204)。そして、認証データ保持部1500は、認証データ[KPp1/CP1]KPaを出力し(ステップS206)、コントローラ1109は、メモリカードインタフェース1200を介してメモリカード110へ認証データ[KPp1/CP1]KPaを入力する(ステップS208)。

【0141】そうすると、メモリカード110は、認証データ[KPp1/CP1]KPaを受理し、復号処理部1408は、受理した認証データ[KPp1/CP1]KPaを、KPa保持部1414に保持された公開認証鍵KPaによって復号し(ステップS210)、コントローラ1420は復号処理部1408における復号処理結果から、認証処理を行なう。すなわち、認証データ[KPp1/CP1]KPaが正規の認証データであるか否かを判断する認証処理を行なう(ステップS212)。復号できなかった場合、ステップS260へ移行し、再生動作は終了する。認証データが復号できた場合、コントローラ1420は、セッションキー発生部1418を制御し、セッションキー発生部1418は、再生セッション用のセッションキーKs2を発生させる(ステップS214)。そして、暗号処理部1410は、セッションキー発生部1418からのセッションキーKs2を、復号処理部1408で復号された公開暗号鍵KPp1によって暗号化した{Ks2}Kp1をバスBS4へ出力する。そうすると、コントローラ1420は、インタフェース1424および端子1426を介してメモリカードインタフェース1200へ{Ks2}Kp1を出力する(ステップS216)。携帯電話機100のコントローラ1109は、メモリカードインタフェース1200を介して{Ks2}Kp1を取得する。そして、コントローラ1109は、{Ks2}Kp1をバスBS2を介してコンテンツ再生回路1550の復号処理部1504へ与え(ステップS218)、復号処理部1504は、Kp1保持部1502から出力された、公開暗号鍵KPp1と対になっている秘密復号鍵Kp1によって{Ks2}Kp1を復号し、セッションキーKs2を暗号処理部1506へ出力する(ステップS220)。そうすると、セッションキー発生部1508は、再生セッション用のセッションキーKs3を発生させ、

セッションキーKs3を暗号処理部1506へ出力する(ステップS222)。暗号処理部1506は、セッションキー発生部1508からのセッションキーKs3を復号処理部1504からのセッションキーKs2によって暗号化して{Ks3}Ks2を出力し(ステップS224)、コントローラ1109は、バスBS2およびメモリカードインタフェース1200を介して{Ks3}Ks2をメモリカード110へ出力する(ステップS226)。

【0142】そうすると、メモリカード110の復号処理部1412は、端子1426、インタフェース1424、およびバスBS4を介して{Ks3}Ks2を入力する。復号処理部1412は、セッションキー発生部1418によって発生されたセッションキーKs2によって{Ks3}Ks2を復号して、再生端末100で発生されたセッションキーKs3を受理する(ステップS228)。

【0143】携帯電話機100のコントローラ1109は、メモリカード110から事前に取得した再生リクエスト曲のライセンス管理ファイルからライセンスの格納されているエントリ番号を取得し(ステップS230)、メモリカードインタフェース1200を介してメモリカード110へ取得したエントリ番号とライセンスの出力要求を出力する(ステップS232)。

【0144】メモリカード110のコントローラ1420は、エントリ番号とライセンスの出力要求とを受理し、エントリ番号によって指定された領域に格納されたライセンスを取得する(ステップS234)。

【0145】そして、コントローラ1420は、アクセス制限情報ACmを確認する(ステップS236)。

【0146】ステップS236においては、メモリのアクセスに対する制限に関する情報であるアクセス制限情報ACmを確認することにより、具体的には、再生回数を確認することにより、既に再生不可の状態である場合には再生動作を終了し、アクセス制限情報の再生回数に制限がある場合にはアクセス制限情報ACmの再生回数を変更した(ステップS238)後に次のステップ(ステップS240)に進む。一方、アクセス制限情報ACmの再生回数によって再生が制限されていない場合には、ステップS238はスキップされ、アクセス制限情報ACmの再生回数は変更されることなく処理が次のステップ(ステップS240)に進行される。

【0147】ステップS236において、当該再生動作において再生が可能であると判断された場合には、メモリ1415のライセンス領域1415Aに記録された再生リクエスト曲のライセンス鍵Kc1および再生制御情報ACpがバスBS4上に出力される(ステップS240)。

【0148】得られたライセンス鍵Kcと再生制御情報ACpは、切換スイッチ1446の接点Pfを介して暗

号化処理部1406に送られる。暗号化処理部1406は、切換スイッチ1442の接点Pbを介して復号処理部1412より受けたセッションキーKs3によって切換スイッチ1446を介して受けたライセンス鍵Kc1と再生制御情報ACpとを暗号化し、(Kc1/ACp) Ks3をバスBS4に出力する(ステップS240)。

【0149】バスBS4に出力された暗号化データは、インタフェース1424、端子1426、およびメモリカードインタフェース1200を介して再生端末102に送出される。

【0150】携帯電話機100においては、メモリカードインタフェース1200を介してバスBS2に伝達される暗号化データ(Kc/ACp) Ks3を復号処理部1510によって復号処理を行ない、ライセンス鍵Kcおよび再生制御情報ACpを受理する(ステップS242、S244)。復号処理部1510は、ライセンス鍵Kc(この場合はライセンス鍵Kc1)をスイッチ1511へ出力する。

【0151】また、復号処理部1510は、再生制御情報ACpをバスBS2に出力する。コントローラ1109は、バスBS2を介して、再生制御情報ACpを受理して再生の可否の確認を行なう(ステップS246)。

【0152】ステップS246においては、再生制御情報ACpによって再生不可と判断される場合には、端子1512にライセンス鍵Kciを出力するようにスイッチ1511に指示し、Kc保持部1514はライセンス鍵Kciを保持する。

【0153】このようにして、Kc保持部1415にライセンス鍵Kc1が保持され、「再生許諾」の処理が終了すると、暗号化コンテンツデータ{Dc1} Kc1が再生可能となる。一方、ステップS212、S236およびS246によって分岐し、Kc保持部1415にライセンス鍵Kc1が保持されないまま「再生許諾」が終了すると、暗号化コンテンツデータ{Dc1} Kc1が再生できない。

【0154】したがって、たとえ暗号化コンテンツデータ{Dc} Kcの一部である試聴領域{Dc1} Kc1のみの再生であっても正規のライセンスを所持しないユーザが再生することはできない構成になっている。もちろん、暗号化コンテンツデータ{Dc} Kcを何らかの手段で取得し、その取得した暗号化コンテンツデータ{Dc} Kcをコピーしたものであってもよい。試聴用ライセンスを配信サーバ10から取得すれば暗号化コンテンツデータ{Dc} Kcを再生可能である。

【0155】また、試聴においては試聴用ライセンスしか保持しないため、ライセンス鍵Kc2にて復号するように暗号化された試聴領域外のブロック、すなわち、本体領域{Dc2} Kc2は本体用ライセンスを取得しない限り、再生することはできない。

【0156】[本体用ライセンスの配信] 次に、ステップS30における本体用ライセンスのダウンロードについて詳細に説明する。本体用ライセンスのダウンロードは、試聴用ライセンスのダウンロードにおける処理と同様に、図10および図11のフローチャートに従って処理される。この場合、ライセンス鍵Kc2を含むライセンスのダウンロードであることから、ライセンス購入条件ACには本体用ライセンスの購入であることを示す情報が含まれている。また、フローチャートにおけるライセンス鍵を区別する識別子iをi=2、すなわちライセンス鍵KciをKc2に読替えればよく、説明が重複するので説明を省略する。

【0157】ここでは、本体用ライセンスを取得した後も、暗号化コンテンツデータの再生にはライセンス鍵Kc1を含む試聴用ライセンスを用いて再生するように説明したが、試聴用ライセンスにはアクセス制御情報ACmに含まれる再生回数制限を利用し、例えば、3回程度の回数制限を加えた上で、無償で配信し、本体用ライセンスとして2つのライセンス、すなわち、ライセンス鍵Kc1を含むライセンスとライセンス鍵Kc2を含むライセンスを同時に配信を行っても同様なサービスを提供することができる。この場合、携帯電話機100は、図9のステップS30において2つのライセンスの配信を受ける。つまり、図10および図11に示すフローチャートを2回処理することで取得することができる。

【0158】[再生] ステップS30によって本体用ライセンスをダウンロードし、2つのライセンスをメモリカード110に格納した後に、2つのライセンス鍵Kc1、Kc2を用いて暗号化コンテンツデータ{Dc} Kcを再生する処理について説明する。ここでは、説明を簡単にするためにライセンス鍵Kc1はKc保持部1514に、ライセンス鍵Kc2はライセンス保持部1515に保持されるものとして説明するが、これに限定されるものではなく逆であってもよい。

【0159】図3を参照して、暗号化コンテンツデータ90を再生する場合について説明する。コントローラ1109は、暗号化コンテンツデータ90に対する付加情報Dc-infを参照して、暗号化コンテンツデータ90において試聴用領域91に属するブロックと本体用領域92に属するブロックを特定する。

【0160】次に、再生順序に従って最初のブロックを再生するために必要なライセンス鍵Kc2をKc保持部1515に保持するための「再生許諾」を図12のフローチャートに従って行なう。この場合、図12のフローチャートにおけるライセンス鍵を区別する識別子iをi=2、すなわちライセンス鍵KciをKc2に読替えればよく、試聴再生における「再生許諾」と同様であるため説明を省略する。

【0161】続いて、スイッチ1518に対して端子1517を選択して、Kc保持部1515に保持されてい

るライセンス鍵Kc2を出力するように指示し、暗号化コンテンツデータ90を構成するブロックを再生順に従ってメモリカード110から読出して復号処理部1519に供給する。さらに、コントローラ1109は、暗号化コンテンツデータ90を構成するブロックを、コンテンツデータの再生が連続して行なわれるように復号処理部1519に供給しつつ、その処理の空き時間を利用して、もう一つのライセンス鍵であるライセンス鍵Kc1をKc保持部1514に保持させる「再生許諾」を試聴用領域91に属するブロックの供給が開始される以前に行なう。ライセンス鍵Kc1に対する「再生許諾」は試聴における再生を行なう場合の「再生許諾」と同様であるので説明は省略する。

【0162】そうすると、コントローラ1109は、暗号化コンテンツデータ90を構成するブロックをメモリカード110から読み出して、再生順に供給し、試聴用領域91に達すると、スイッチ1518に対して端子1516を選択してKc保持部1514に保持されているライセンス鍵Kc1を復号処理部1519に出力するように指示し、引き続いて、暗号化コンテンツデータ90を構成するブロックを再生順に従ってメモリカード110から読出して復号処理部1519に供給する。

【0163】そして、再び、本体用領域92に達すると、再びスイッチ1518に対して端子1517を選択してKc保持部1515に保持されているライセンス鍵Kc2を復号処理部1519に出力するように指示し、引き続いて、暗号化コンテンツデータ90を構成するブロックを再生順に従ってメモリカード110から読出して復号処理部1519に供給する。すべてのブロックが供給されると、暗号化コンテンツデータ90の再生が終了する。

【0164】さらに、図3を参照して、暗号化コンテンツデータ93を再生する場合について説明する。暗号化コンテンツデータ93では、再生順に従うと、最初にライセンス鍵Kc1によって再生する試聴用領域94が存在する。従って、まず、ライセンス鍵Kc1をKc保持部1514に保持させる「再生許諾」を行なう。次いで、コントローラ1109は、暗号化コンテンツデータ93を構成するブロックをメモリカード110から読み出して、再生順に復号処理部1519に供給する。さらに、コントローラ1109は、暗号化コンテンツデータ93を構成するブロックを、コンテンツデータの再生が連続して行なわれるように復号処理部1519に供給しつつ、その処理の空き時間を利用して、もう一つのライセンス鍵であるライセンス鍵Kc2をKc保持部1515に保持させる「再生許諾」を本体用領域95に属するブロックの供給が開始される以前に行なう。

【0165】本体用領域95に達すると、スイッチ1518に対して、端子1517を選択してKc保持部1514に保持されているライセンス鍵Kc2を復号処理部

1519に出力するように指示し、引き続いて、暗号化コンテンツデータ93を構成するブロックを再生順に従ってメモリカード110から読出して復号処理部1519に供給する。すべてのブロックが供給されると、暗号化コンテンツデータ93の再生が終了する。

【0166】図1に示すパーソナルコンピュータ50が配信サーバ10またはCD-ROM60から暗号化音楽データ{Dc}Kcのみを取得して、カードライタ80を介してメモリカード110に格納することもできる。この場合、図9のステップS10における暗号化コンテンツデータのダウンロード処理が省略される。

【0167】また、図1に示すパーソナルコンピュータ50は、試聴用の暗号化音楽データ{Dc1}Kc1、本体用の暗号化音楽データ{Dc2}Kc2、およびライセンス鍵Kc1を含む試聴用ライセンスを配信サーバ10またはCD-ROM60から取得して、カードライタ80を介してメモリカード110に格納することができる。この場合、図9のステップS10をパーソナルコンピュータ50が行ない、パーソナルコンピュータ50からカードライタ80を介したメモリカード110へのライセンスの格納は、図10および図11に示すフローチャートに従って行なわれる。この場合、パーソナルコンピュータ50は、図10および図11における配信サーバ10と携帯電話機100の機能を果たす。そして、携帯電話機100のユーザは、カードライタ80からメモリカード110を抜き、携帯電話機100に装着し、図12に示すフローチャートに従って暗号化音楽データ{Dc}Kcの試聴領域{Dc1}Kc1を試聴する。その後、暗号化音楽データ{Dc}Kcを聴きたいとき、携帯電話機100によって配信サーバ10から本体用の暗号化音楽データ{Dc2}Kc2を復号するためのライセンス鍵Kc2を図10および図11に示すフローチャートに従ってダウンロードする。そして、携帯電話機100は、ユーザの再生要求に応じて、2つのライセンス鍵Kc1、Kc2を用いて暗号化音楽データ{Dc}Kcの全てを再生する。また、説明をし省略したが、配信サーバ10から試聴用ライセンスの取得、あるいはCD-ROM60への試聴用ライセンスの記録および試聴用ライセンスの読出しは暗号技術を用いて安全性が確保されているものとする。ただし、ここでは、その方法については限定しないものとする。さらに、本体用ライセンスをコンピュータ50にて配信サーバ10から受信してカードライタ80を介してメモリカード110に格納することも可能である。

【0168】このように、携帯電話機100は、各種の経路から暗号化音楽データ{Dc}Kc、およびライセンス鍵Kc1、Kc2をそれぞれ含む2つのライセンスを受信してメモリカード110に記録する。したがって、携帯電話機100のユーザが暗号化音楽データ{Dc}Kcの全てを再生できる状態でのダウンロードを希

望したとき、メモリカード110には、最終的に、暗号化音楽データ[Dc]Kc、およびライセンス鍵Kc1、Kc2をそれぞれ含む2つのライセンスが格納される。

【0169】上記においては、暗号化コンテンツデータが音楽データを暗号化した暗号化コンテンツデータである場合について説明したが、暗号化コンテンツデータが他の朗読データ、教材データ、およびビデオデータ等であっても上述した方法によって暗号化コンテンツデータのダウンロード、試聴、試写および再生を行なう。

【0170】本発明の実施の形態によれば、複数のブロックに分割された暗号化コンテンツデータと、複数のブロックに含まれる暗号化データを復号するための複数のライセンスとを配信するので、各ブロックを異なるライセンスによって復号および再生できる。その結果、配信されるライセンスに応じて課金料金を設定できる。

【0171】今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【0172】

【発明の効果】本発明によれば、複数のブロックに分割された暗号化コンテンツデータと、複数のブロックに含まれる暗号化データを復号するための複数のライセンスとを配信するので、各ブロックを異なるライセンスによって復号および再生できる。

【図面の簡単な説明】

【図1】 データ配信システムを概念的に説明する概略図である。

【図2】 図1に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図3】 暗号化コンテンツデータのフォーマットを示す図である。

【図4】 暗号化コンテンツデータの生成方法を説明するための図である。

【図5】 図1に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図6】 図1に示すデータ配信システムにおける配信サーバの構成を示す概略ブロック図である。

【図7】 図1に示すデータ配信システムにおける携帯電話機の構成を示す概略ブロック図である。

【図8】 図1に示すデータ配信システムにおけるメモリカードの構成を示す概略ブロック図である。

【図9】 図1に示すデータ配信システムにおける配信動作の全体構成を説明するためのフローチャートである。

【図10】 図9に示すライセンスの配信動作をさらに詳細に説明するための第1のフローチャートである。

【図11】 図9に示すライセンスの配信動作をさらに詳細に説明するための第2のフローチャートである。

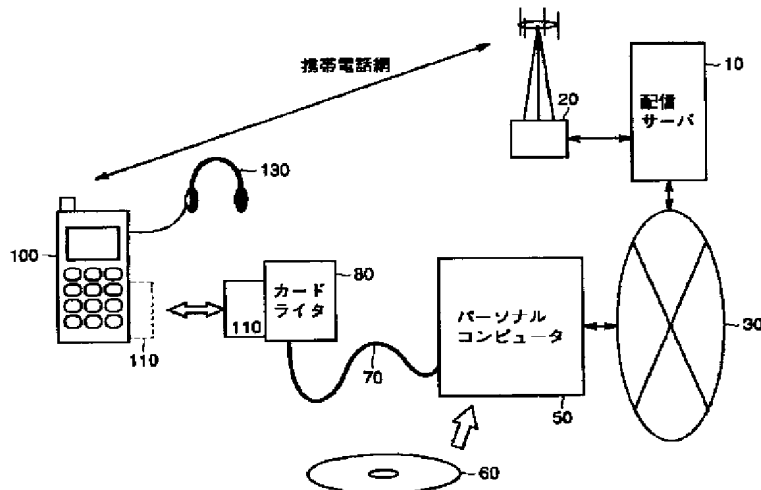
【図12】 再生許諾動作におけるライセンス鍵の読出を詳細に説明するためのフローチャートである。

【図13】 暗号化コンテンツデータの別のフォーマットを示す図である。

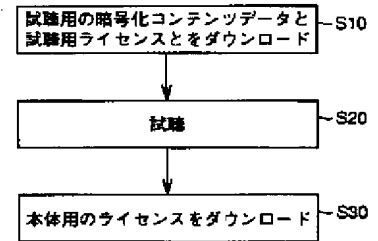
【符号の説明】

10 配信サーバ、20 配信キャリア、30 インターネット網、50 パーソナルコンピュータ、60 CD、70 USBケーブル、84、90、93、96、97 暗号化コンテンツデータ、81 源データ、82 ブロックデータ、83、91、92、94、95、842、844、846 暗号化音楽データ100 携帯電話機、110 メモリカード、130 ヘッドホン、302 課金データベース、304 情報データベース、307 メニューデータベース、308 配信記録データベース、310 データ処理部、312、320、1404、1408、1412、1422、1504、1510、1519 復号処理部、313 認証鍵保持部、315 配信制御部、316、1418、1508 セッションキー発生部、318、326、328、1406、1410、1417、1506 暗号処理部、350 通信装置、841、843、845、971、972 暗号化データ、961~967 領域、1109、1420 コントローラ、1426、1512、1513、1516、1517、1522 端子、1101 アンテナ、1102 送受信部、1103 マイク、1104 AD変換器、1105 音声符号化部、1106 音楽再生部、1108 スピーカ、1110 表示パネル、1111 操作パネル、1200 メモリカードインタフェース、1400、1500 認証データ保持部、1402 Km c保持部、1414 KPa保持部、1415 メモリ、1415A ライセンス領域、1415B データ領域、1416 KPmc保持部、1421 Km保持部、1424 インタフェース、1442、1446 切換スイッチ、1502 Kp1保持部、1520 音楽再生部、1107、1521 DA変換器、1514、1515 Kc保持部、1550 コンテンツ再生回路。

【図1】



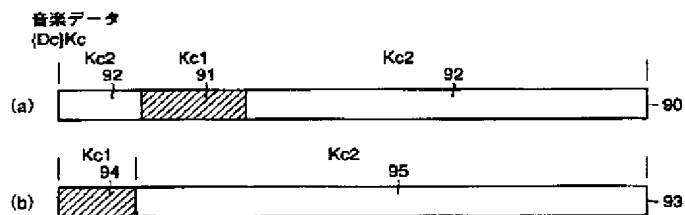
【図9】



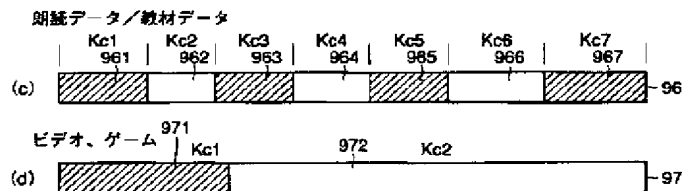
【図2】

記号	種類	属性	特性
Dc	コンテンツデータ	コンテンツ固有	例：音楽データ、朗読データ、教材データ、画像データ Kcにて復号可能な暗号化コンテンツデータ {Dc}Kcとして配信され、メモリカードに保持される
Dc-inf	付加情報	コンテンツ固有	Dcに付随する平文データ。
Kc	ライセンス	コンテンツ固有	ライセンス 暗号化コンテンツデータを復号する復号鍵
ACm/ACp	ライセンス	ライセンス固有	制限情報 再生やライセンスの取り扱いに対する制限事項
ライセンスID	ライセンス	ライセンス固有	ライセンスを特定するための管理コード
コンテンツID	ライセンス	コンテンツ固有	コンテンツを特定するための管理コード
ライセンス	ライセンス	ライセンス固有	Kc+ACm+ACp+ライセンスID+コンテンツIDの総称

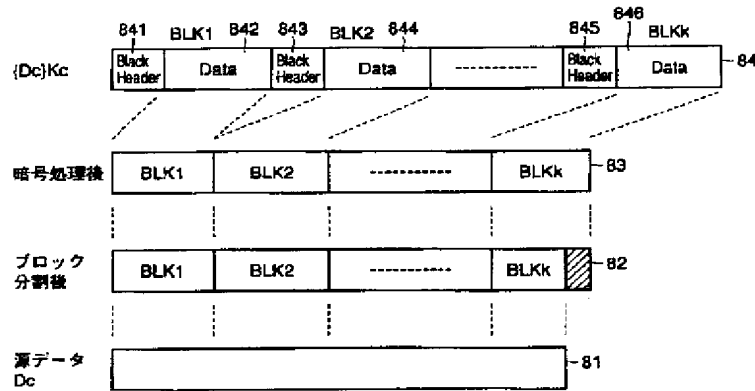
【図3】



【図13】

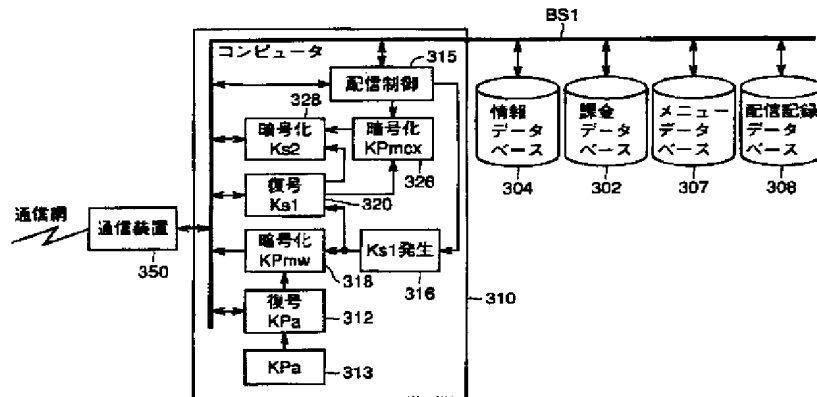


【図4】



【図6】

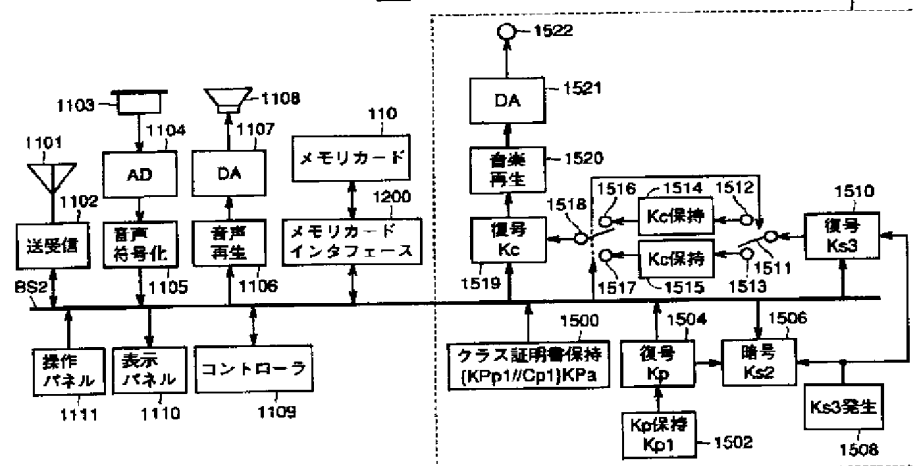
10



【図7】

100

1550



【図5】

	記号	種類	属性	特性
配信サーバ	KPa	公開認証鍵	システム 共通	認証局にて認証データを復号する鍵
	Ks1	共通鍵	セッション 固有	メモリカードへのライセンス配信ごとに発生
メモリカード	KPa	公開認証鍵	システム 共通	認証局にて認証データを復号する鍵 配信サーバのKPaと同一
	KPmw	公開暗号鍵	クラス固有	証明書Cmwとともに認証局にて暗号化された認証データとして保持 wはクラスを識別するための識別子
	Kmw	秘密復号鍵	クラス固有	公開暗号鍵KPmwにて暗号化されたデータを復号する非対称な 復号鍵
	KPmcx	公開暗号鍵	個別	メモリカードごとに異なる。 xはモジュールを識別するための識別子
	Kmcx	秘密復号鍵	個別	公開暗号鍵KPmcxにて暗号化されたデータを復号する非対称な 復号鍵
	Ks2	共通鍵	セッション 固有	配信サーバまたはコンテンツ再生回路間のライセンスの授受ごとに 発生
	Cmw	証明書	クラス 証明書	メモリカードのクラス証明書。認証機能を有する。 (KPmw/Cmw)KPaの形式で出荷時に記録。 *メモリカードのクラスwごとに異なる。
	KPpy	公開暗号鍵	クラス固有	証明書Cmwとともに認証局にて暗号化された認証データとして保持 yはクラスを識別するための識別子
	Kpy	秘密復号鍵	クラス固有	公開暗号鍵KPpyにて暗号化されたデータを復号する非対称な復号鍵
	Ks3	共通鍵	セッション 固有	メモリカード間の再生セッションごとに発生
コンテンツ 再生回路	Cpy	証明書	クラス 証明書	コンテンツ再生デバイスのクラス証明書。認証機能を有する。 (KPpy/Cpy)KPaの形式で出荷時に記録。 *コンテンツ再生デバイスのクラスyごとに異なる。

[illegible]

```

graph TD
    subgraph MemoryCard [メモ리카ード]
        S106[認証データ送信要求の受信]
        S108["{KPm3//Cm3}KPaを出力"]
        S128[ライセンスID//{Ks1}Km3の受信]
        S132["{Ks1}Km3をKm3にて復号し、Ks1の受理"]
        S134[セッション鍵Ks2の生成]
        S138["Ks2bとKPmc4をKs2にて暗号化し、{Ks2//KPmc4}Ks1を出力"]
    end

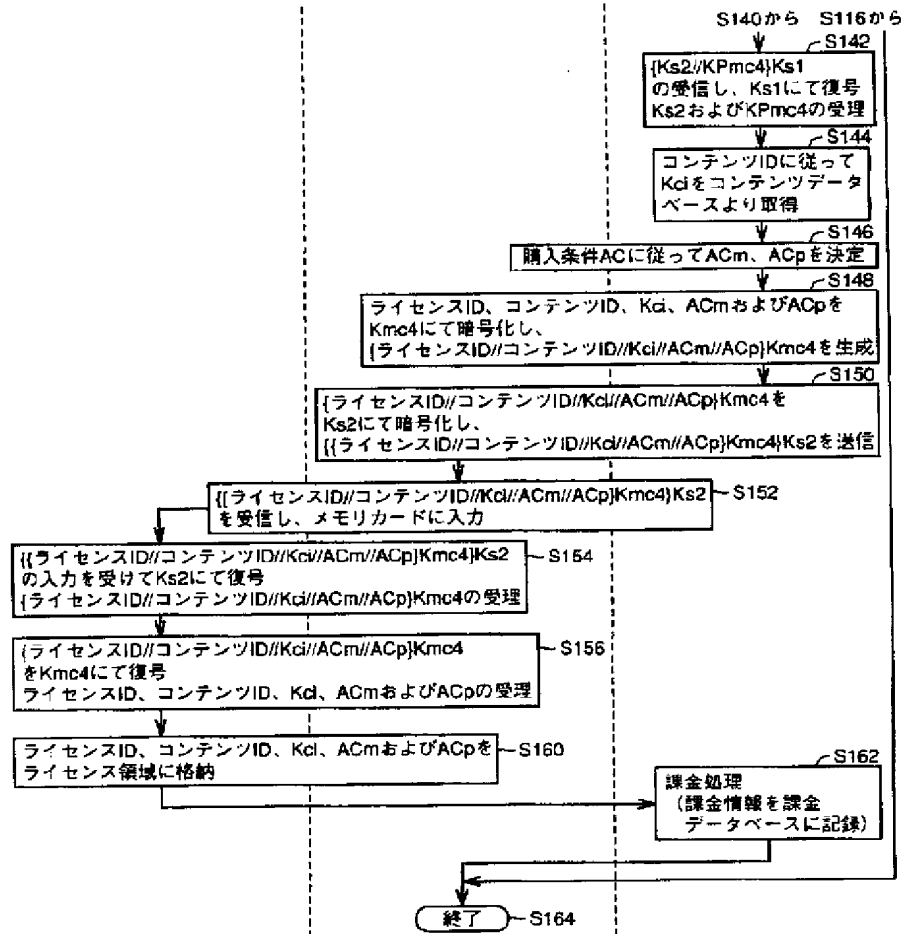
    subgraph Controller [コントローラ]
        Start([開始])
        S100[コンテンツID指示による配信リクエスト]
        S102[ライセンスの購入条件ACの入力]
        S104[メモリカードへ認証データ出力要求]
        S110[コンテンツID//AC//{KPm3//Cm3}KPaを配信サーバへ送信]
        S126[ライセンスID//{Ks1}Km3を受信し、メモリカードに入力]
        S140["{Ks2//KPmc4}Ks1を受信し、配信サーバへ送信"]
    end

    subgraph DistributionServer [配信サーバ]
        S112[コンテンツID//AC//{KPm3//Cm3}KPaを受信]
        S114["{KPm3//Cm3}KPaをKPaにて復号"]
        S116{KPm3の受理}
        S118[セッション鍵Ks1の生成]
        S120["Ks1をKPm3にて暗号化し、{Ks1}Km3の生成"]
        S122[ライセンスIDの生成]
        S124[ライセンスID//{Ks1}Km3の送信]
        S142[ ]
        S144[ ]
    end

    Start --> S100
    S100 --> S102
    S102 --> S104
    S104 --> S106
    S106 --> S108
    S108 --> S110
    S110 --> S112
    S112 --> S114
    S114 --> S116
    S116 -- No --> S142
    S116 -- Yes --> S118
    S118 --> S120
    S120 --> S122
    S122 --> S124
    S124 --> S126
    S126 --> S128
    S128 --> S132
    S132 --> S134
    S134 --> S138
    S138 --> S140
    S140 --> S144
    S142 --> S144
  
```

The flowchart illustrates the process of content distribution and license management. It involves three main components: the Memory Card (メモ리카ード), the Controller (コントローラ), and the Distribution Server (配信サーバ). The process begins with the Controller sending a content distribution request (S100) and receiving a license purchase condition (S102). The Controller then sends an authentication data output request (S104) to the Memory Card, which outputs authentication data (S106, S108). The Controller sends this data to the Distribution Server (S110). The Distribution Server receives the data (S112), decodes it (S114), and checks if the KPm3 is accepted (S116). If not, it proceeds to S142. If yes, it generates a session key Ks1 (S118), encrypts it with KPm3 (S120), generates a license ID (S122), and sends the license ID and Ks1 (S124). The Controller receives this (S126) and sends the license ID and Ks1 to the Memory Card (S128). The Memory Card receives this (S128), decrypts Ks1 (S132), generates a session key Ks2 (S134), encrypts Ks2b and KPmc4 with Ks2 (S138), and outputs the result (S140). The Controller receives this (S140) and sends it to the Distribution Server (S144). The Distribution Server receives this (S144) and proceeds to S142.

【図11】



【図12】

